Universidade de Aveiro
2010
Departamento de Economia, Gestão e Engenharia Industrial

ALBERTINA DA CUNHA COUTO FERREIRA

A GESTÃO DE RISCO APLICADA À AUDITORIA INTERNA

Universidade de Aveiro
2010
Departamento de Economia, Gestão e Engenharia Industrial

ALBERTINA DA CUNHA COUTO FERREIRA

A GESTÃO DE RISCO APLICADA À AUDITORIA INTERNA

Dissertação apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Contabilidade e Auditoria, realizada sob a orientação científica da Doutora Helena Coelho Inácio, Professor Ajunto do Departamento de ISCAA da Universidade de Aveiro

Dedico este trabalho ao meu marido, José António, e aos meus filhos, José António e José Miguel, pelo apoio e pela força que me deram para realizar este trabalho e acima de tudo pela compreensão de se verem privados da minha companhia e atenção.

o júri

presidente

Prof. Doutora Maria de Fátima Marques Teixeira Lopes Pinho
professora adjunta da Universidade de Aveiro

Prof. Doutor Manuel Emílio Mota de Almeida Delgado Castelo Branco
professor auxiliar da Faculdade de Economia da Universidade do Porto

Prof. Doutora Helena Coelho Inácio
professora adjunta da Universidade de Aveiro

agradecimentos

Agradeço à minha orientadora, Doutora Helena Inácio Coelho, pela disponibilidade demonstrada e pela preciosa ajuda na elaboração deste trabalho.

Quero também agradecer aos meus colegas e amigos, Dr. João Machado, Dr. Armando Lopes, Dr. Paulo Rodrigues e D. Candida Castro, pelo apoio prestado.

palavras-chave Gestão de Risco, Risco, Medidas, Auditoria Interna, Processo de Compras.

resumo

A globalização da economia, o aumento da concorrência, as expectativas cada vez maiores dos consumidores, a crise económica mundial a que assistimos, estão a afectar as organizações, expondo-as a uma grande variedade de riscos, que podem afectar a concretização dos seus objectivos. Deste modo, as organizações devem conhecer os riscos que ameaçam o seu negócio, de modo a implementar medidas adequadas que mitiguem estes mesmos riscos e assim não coloquem em causa o cumprimento dos objectivos definidos para a organização.

Neste contexto actual, consideramos que a nova visão da Auditoria Interna é uma mais-valia para a criação de valor da organização, uma vez que, deixa de se preocupar apenas com factos passados e controlos e passa a incluir no seu trabalho a identificação, análise e avaliação dos riscos (visão futura), contribuindo para a obtenção de "uma segurança razoável" de que os principais objectivos de negócio serão concretizados.

Neste contexto, partindo do modelo de gestão de risco da norma Australiana/Neozelandesa (AS/NZS 4360:2004) e do COSO ERM, aplicamos a metodologia da gestão de risco a um processo de compras, cujo objectivo é demonstrar como é que se pode incorporar a gestão de risco nos trabalhos realizados pela Auditoria Interna incluindo a apresentação de ferramentas que suportam o trabalho realizado e os resultados obtidos.

O trabalho apresentado nesta dissertação seguiu as fases definidas na norma AS/NZS 4360:2004, tendo-se iniciado pelo estabelecimento do contexto, passando pela identificação, analise e avaliação dos riscos e dos controlos, determinando-se assim o risco residual. Por fim, são identificadas as falhas de controlo e efectuadas as recomendações pela Auditoria Interna que visam reduzir a exposição do processo de compras, sub-processo compras orçamento, ao risco analisado.

De referir que a fase da comunicação e consulta se relaciona com todas as fases do processo de gestão de risco. A fase da monitorização e revisão não foi englobada no âmbito deste trabalho. Todo este trabalho está suportado em mapas de trabalho, dos quais destacamos as matrizes de risco absoluto e risco residual, matriz de análise de riscos e controlos e matriz de tratamento de riscos.

keywords Risk Management, Risk, Internal, Audit, Procurement.

abstract

Nowadays there are several issues affecting organizations, the globalization of the economy, the increase of competitiveness among companies, and the world crisis that we are now dealing with. Those facts are exposing companies to higher risks which may compromise the objectives set by Management.
Therefore companies should know the risks they are facing so they can implement the necessary measures to mitigate those risks and accomplish their objectives.

This new paradigm of the Internal Audit function adds up value for the organization, since it concentrates not in the past but in the future, including in their work the identification, analysis and evaluation of risks relating them with the main objectives set by the company.

In this context, based on the risk management framework AS/NZS 4360:2004 and in COSO ERM, it was applied in this work the risk management methodology to an audit work of a procurement process with the objective of demonstrating the application of risk management techniques in the internal audit work, including the presentation of the support files and the results achieved.

The work performed followed the phases defined in the risk management model AS/NZS 4360:2004, starting by establishing the context, followed by the identification, analysis and evaluation of absolute risks, controls in place and the residual risks.
Finally, findings were identified and Internal Audit issued their recommendations that in their perspective would help the company to reduce company risk exposures.
Communication and consultation were contemplated in each phase of risk management process.
Monitoring and Reviewing were not included in the scope of this work.
All work is supported in worksheets, for example, the absolute and residual risks matrix, the risk analysis matrix and the risk treatment matrix.

ÍNDICE GERAL

1.Introdução....1
2. Abordagens da Auditoria Interna....3
2.1. Perspectiva evolutiva da Noção de AI 3
2.2. Controlo Interno 7
2.3. Principais diferenças entre Controlo Interno e Auditoria Interna....11
2.4. As Normas Internacionais para a Prática Profissional de Auditoria Interna 12
3. Gestão de Risco Empresarial 14
3.1. Evolução e Conceito 14
3.2. Risco....16
3.3. Utilizadores da Gestão de Risco 18
3.4. Modelos de Gestão de Risco Empresarial....19
3.4.1. O COSO ERM....19
3.4.2. Norma Australiana / Neozelandesa AS/ NZS 4360:2004....23
3.4.3. Norma de Gestão de Riscos - FERMA....27
3.4.4. O COBIT 28
3.4.5. ISO 31000:2009....30
3.5. Limitações da Gestão de Risco Empresarial....32
4. Metodologia da Auditoria Focalizada na Gestão de Riscos....33
4.1. Processo de Auditoria Interna baseado nos Riscos do Negócio....33
4.2. Principais Objectivos de uma AIBR....34
4.3 Razões para a implementação de uma AIBR....35
4.4. O Papel do Auditor Interno na Gestão de Riscos 36
4.5.Técnicas utilizadas para medir o risco....39
5. Aplicação prática: a avaliação do risco num processo de compras....43
5.1. Metodologia 43
5.1.1. Objectivos 43
5.1.2. Modelo e fases de aplicação....43
5.1.3. Universo utilizado para aplicação do modelo....52
5.1.4. Pressupostos 52
5.2. Aplicação da avaliação de risco num processo de compras....53
5.2.1. Estabelecimento do Contexto....53
5.2.1.1. Compreender o contexto estratégico....54
5.2.1.1.1. Caracterização do Departamento de Compras....54
5.2.1.1.2. Políticas e Procedimentos internos aplicáveis 56

5.2.1.2. Compreender os processos de negócio 56
5.2.1.2.1. Processos principais e de suporte às Compras 56
5.2.1.2.1.1. Processos principais 58
5.2.1.2.1.2. Processos de suporte às Compras 62
5.2.1.2.2. Enquadramento dos processos na Estrutura Organizativa 63
5.2.1.3. Estabelecer uma linguagem comum 65
5.2.2. Processo de Avaliação dos Riscos 68
5.2.2.1. Identificação dos riscos - Risco Absoluto 68
5.2.2.2. Análise dos riscos 72
5.2.2.3. Avaliar os riscos 76
5.2.3. Tratar os riscos 80
5.2.4. Ficha de análise de riscos e controlos 82
5.3. Limitações da aplicação prática 84
5.4. Análise crítica 85
6. CONCLUSÃO 88
BIBLIOGRAFIA 90
ANEXOS 95

Índice de Quadros

Quadro 1: Comparação entre o Velho e o Novo Paradigma 5
Quadro 2: Principais diferenças entre CI e AI 11
Quadro 3: Normas de Desempenho IIA, relevantes na GR 13

Índice de Figuras

Figura 1: Ideograma Chinês (Risco/Crise) 17
Figura 2: Principais interessados 19
Figura 3: Cubo do COSO ERM 21
Figura 4: Processo de Gestão de Risco 23
Figura 5: Matriz de Risco 40
Figura 6: Exemplo de Matriz de Riscos..... 45
Figura 7: Excerto Mapa dos Riscos Inerentes 48
Figura 8: Matriz Risco Inerente..... 48
Figura 9: Passagem da Matriz de Risco Inerente para a Matriz de Risco Residual 50
Figura 10: Estabelecimento do Contexto 54
Figura 11: Processos principais e processo de suporte – Compras 57
Figura 12: Fluxograma do Processo Compras Orçamento 59
Figura 13: Fluxograma do Processo de Compras de Serviços 60
Figura 14: Fluxograma do Processo de Compras Pontuais 61
Figura 15: Fluxograma do processo de Compras Delegadas 62
Figura 16: Enquadramento dos processos de Compras na Organização 64
Figura 17: Fontes de Incerteza 65
Figura 18 . Matriz de Riscos de Negócio 68
Figura 19: Matriz de Risco Inerente dos Processos de Compras 70
Figura 20: Tabela dos riscos mais importantes (Relativas aos cinco riscos inerentes mais significativos) (Impacto> 3) 71
Figura 21: Tabela do Processo Auditado 71
Figura 22: Excerto da Matriz de Risco Inerente dos Processos Auditados 72
Figura 23: Exemplo de Matriz de Análise dos Controlos ao Processo Analisado (excerto) 75
Figura 24: Matriz de Risco Residual dos Processos Auditados 78
Figura 25: Tabela de frequência das ocorrências (Relativas aos riscos residuais mais significativos, com impacto> 3) 79
Figura 26: Ficha de análise de Riscos e Controlos 83

GLOSSÁRIO DE SIGLAS

AI – Auditoria Interna

AIBR – Auditoria Interna Baseada no Risco

AICPA – American Institute of Certified Public Accountants

CI – Controlo Interno

COBIT – Control Objectives for Information and Related Technology

COSO – The Committee of Sponsoring Organizations of the Treadway Commission

ERM – Enterprise Risk Management

FERMA - Federation of European Risk Management Associations

IIA – The Institute of Internal Auditors

IFAC – International Federation of Accountants

IGIT– IT Governance Institute

IPAI – Instituto Português de Auditores Internos

IRAM – Instituto Argentino de Normalización e Certificación

ISA – International Standards on Auditing

ISACA – Information Systems Audit and Control Association

SEC – Securities and Exchange Commission

SOX – Lei Sarbanes-Oxley

TI - Tecnologia de Informação

1.Introdução

A velocidade de mudança, a complexidade crescente da economia associada à crise económica mundial que estamos a atravessar, as expectativas cada vez maiores dos consumidores, a agressividade da concorrência, as consequências dramáticas que podem advir das falhas de controlo, a rápida evolução da tecnologia, entre outros factores, estão a afectar as organizações, expondo-as a uma grande variedade de riscos. Os riscos empresariais podem assumir várias formas e o seu impacto nos stakeholders (accionistas, clientes, fornecedores, colaboradores, entre outros) pode ser inesperado, rápido e atingir grandes proporções. Deste modo, as Organizações devem conhecer os riscos que ameaçam o seu negócio, de modo a implementar medidas adequadas que mitiguem estes mesmos riscos e que evitem colocar em causa a concretização dos objectivos e até mesmo a continuidade do negócio.

Tendo em consideração o contexto actual, consideramos que a nova visão da Auditoria Interna é uma mais-valia para a criação de valor da organização. Neste sentido, referimo-nos à evolução do paradigma da Auditoria Interna, nomeadamente ao facto da Auditoria Interna deixar de se preocupar apenas com factos passados e controlos e passar a incluir no seu trabalho a identificação, análise e avaliação dos riscos (visão futura), o que contribui para a obtenção de "uma segurança razoável" de que os principais objectivos de negócio serão concretizados.

A visão moderna diz-nos que as empresas que melhor responderão às mutações que rapidamente estão a acontecer no mercado global, são aquelas que compreendem desde já, de uma forma mais esclarecida, os seus riscos e que alinham essa assumpção de riscos com aquilo que melhor sabem fazer.

É neste enquadramento que entendemos ser relevante conhecer a forma como a Auditoria Interna pode articular-se com a Gestão de Risco com vista à criação de valor para a empresa.

Assim, com o objectivo de mostrar a aplicabilidade de um modelo de gestão de risco nos processos de Auditoria Interna, apresentamos uma aplicação prática do modelo de risco resultante da conjugação entre a Norma Australiana/Neozelandesa 4360:2004 e o COSO ERM a um dos processos de uma empresa – o processo de compra.

A nossa dissertação encontra-se dividida em cinco capítulos que passamos a apresentar de forma resumida.

No primeiro capítulo apresentamos o enquadramento do tema, o principal objectivo, assim como o conteúdo de cada capítulo.

No segundo capitulo, apresentamos a evolução da actividade da Auditoria Interna, focando-se a mudança de paradigma, assim como as diferenças entre a Auditoria Interna e Controlo Interno.

No terceiro capítulo, fizemos uma abordagem à gestão de risco nas organizações, bem como, apresentamos vários modelos de gestão de risco, considerados a nível mundial como os mais conceituados e que representam as melhores práticas nesta área.

No quarto capítulo, abordamos a metodologia da Auditoria Interna focalizada na gestão de risco, nomeadamente no que diz respeito aos objectivos e ao papel do Auditor Interno na gestão de riscos.

Por último, no quinto capítulo, apresentam-se as principais conclusões obtidas no nosso estudo.

2. Abordagens da Auditoria Interna

2.1. Perspectiva evolutiva da Noção de AI

Durante muitas décadas a Auditoria Interna foi entendida como uma actividade que visava essencialmente a avaliação da fiabilidade dos controlos internos, frequentemente, designada de "o controlo dos controlos", ou seja, tinha como principal função salvaguardar os activos da empresa, verificar se os procedimentos instituídos na organização estavam a ser cumpridos e ainda verificar a veracidade da informação financeira.

Não podemos deixar de salientar a importância que teve no desenvolvimento da actividade de Auditoria Interna, o Institute of Internal Auditors (IIA), criado em 1941. Este organismo tem membros em vários países o que vai permitindo, por um lado, a divulgação das melhores práticas de Auditoria Interna, por outro, a uniformização da profissão pelos padrões mais elevados. Em Portugal, foi criado em 1992, o Instituto de Auditores Internos (IPAI, também membro do IIA).

Conforme referido por Costa (2007), a aprovação dos "Standards for the Professional Practice of Internal Auditing" em 1978, pelo IIA, também teve um contributo muito positivo na evolução da Auditoria Interna, dado que na introdução se define a Auditoria Interna como "uma função de apreciação independente, estabelecida dentro de uma organização, como um serviço para a mesma, para avaliar e examinar as suas actividades. O objectivo da Auditoria Interna é o de auxiliar os membros da organização no desempenho eficaz das suas responsabilidades. Com esta finalidade, a Auditoria Interna fornece-lhes análises, apreciações, conselhos e recomendações respeitantes às actividades analisadas" (Costa, 2007:88).

Em Junho de 1999, a noção de Auditoria Interna foi redefinida pelo IIA, passando a incorporar as mudanças ocorridas na profissão e a orientar os auditores internos para uma actividade mais abrangente, em que se dá maior relevo à questão do valor acrescentado que é dado pela Auditoria Interna à organização. A Auditoria Interna passou a ser definida como "uma actividade independente de garantia e de consultoria, destinada a acrescentar valor e a melhorar as operações de uma organização. Assiste a organização na consecução dos seus objectivos, através de

uma abordagem sistemática e disciplinada, para a avaliação e melhoria da eficácia dos processos de gestão de risco, controlo e governação" (IIA,1999).

Esta alteração mostra a mudança que tem vindo a acontecer ao longo dos anos na actividade de Auditoria Interna, em que estamos a passar de um trabalho essencialmente focado em factos passados, para um trabalho que se foca no presente e no futuro, acrescentando deste modo maior valor à organização. Esta nova focalização da Auditoria Interna veio dar lugar ao que se designa, frequentemente, Auditoria Interna Base Risco (AIBR).

Na mesma linha de pensamento está Junior (2005) ao referir que inicialmente, a função de Auditoria Interna estava ancorada na análise das transacções com o objectivo de evitar fraudes, depois focou-se na avaliação dos controlos internos com o objectivo de reduzir os erros e actualmente está centrada na avaliação dos controlos internos numa óptica de risco com a finalidade de optimizar o processo de gestão, isto é, de criar valor aos accionistas.

De acordo com Sousa (2007), a Auditoria Interna deverá deixar de estar focalizada na garantia da correcta escrituração do passado, para estar mais comprometida com a Gestão, de modo a que os objectivos e metas da empresa sejam alcançados.

Deste modo, a AIBR passou a utilizar todas as técnicas de gestão de riscos, incluindo outras técnicas de gestão além de actividades de controlo.

A este propósito Pinheiro (2008), refere que a Auditoria Interna deverá evoluir para a Auditoria de Gestão ("Value For Money Audit"), com o objectivo de acompanhar o desenvolvimento e a utilização de métodos de gestão de riscos negativos das empresas e, assim, aumentar o sucesso da função numa óptica de acrescentar valor quer aos processos quer à empresa.

Segundo Morais (2008), fornecer valor à empresa, trata-se de um conjunto de interesses internos e externos que possibilitam um ganho, quer seja monetário ou não.

Os controlos são importantes mas para fornecer valor à empresa a função de Auditoria Interna deve focar-se nos riscos de negócio que podem ser críticos para a sua empresa, conforme refere Lorenzo (2001).

O quadro 1 apresenta um resumo das diferenças nos focos da auditoria em termos gerais, dos testes, relatório e dos resultados de auditoria, entre o velho e o novo paradigma.

Área de Auditoria	Velho Paradigma	Novo Paradigma
Focus de auditoria	Sistemas de controlo interno	Riscos de Negócio
Focus de testes	Actividades de controlo	Actividades de Mitigação de todos os Riscos
Focus de relatório	Adequacidade e eficácia dos controlos internos	Adequacidade e eficácia da Mitigação dos Riscos
Resultados de auditoria	Controlo novo ou melhorado	Mitigação apropriada do Risco

Quadro 1: Comparação entre o Velho e o Novo Paradigma (**Fonte:** Mc Namee, 1997)

A diferença entre estes dois paradigmas reside essencialmente na transferência da focalização do controlo para os riscos. A auditoria, deixou de ser vista como uma mera função de controlo financeiro/contabilístico, passando a preocupar-se com a identificação dos riscos inerentes ao negócio, na identificação das actividades de controlo e avaliação da eficácia das mesmas na mitigação dos riscos, bem como, propor recomendações com o objectivo de implementarem medidas de correcção e melhoria para mitigação do risco, de modo a que os objectivos da organização sejam atingidos. Deste modo, a Auditoria Interna tem como principal objectivo apoiar a gestão de topo a alcançar os objectivos definidos para a organização.

Trata-se de um paradigma diferente, do olhar para a frente, uma auditoria centrada sobre os riscos acrescenta mais valor à organização do que uma auditoria centrada apenas nos controlos e ou somente nos factos passados registados na contabilidade como refere Cocurrullo e Vanca (2002).

De acordo com Almeida (2006), o valor em auditoria traduz-se no desenvolvimento de actividades nos processos e áreas de maior risco das organizações, de modo a reduzir esse risco para níveis aceitáveis e na melhoria do ambiente de controlo interno. Não é mais do que partir do risco inerente elevado para chegar a um risco residual tolerável pela empresa e que não coloque em causa a concretização dos seus objectivos.

Segundo Lorenzo (2001), hoje em dia o Auditor Interno fixa-se no presente e no futuro, nos riscos actuais e nos que hão-de vir, a sua atitude torna-se pró-activa acrescentando maior valor à empresa.

De acordo com McNamee (1997a), a avaliação de riscos permite ao auditor definir um programa de auditoria capaz de testar os controlos mais importantes, ou testar os

controlos com maior detalhe, bem como, ajuda a definir as áreas auditáveis mais críticas, sobre as quais a auditoria se irá debruçar em primeiro lugar.

No seguimento do Enterprise Risk Management (ERM) emitido pelo COSO, o IIA veio esclarecer a posição da Auditoria Interna, considerando que:

> *"*O principal papel da Auditoria Interna no processo de gestão de risco é fornecer segurança objectiva acerca da eficácia das actividades de gestão de risco das organizações, para ajudar a assegurar que os principais riscos do negócio estão a ser geridos de forma apropriada e que o sistema de controlo interno está a funcionar eficazmente" (IIA, 2004:2).

De acordo com McNamee (1997b), a Auditoria Interna baseada em riscos, melhora o modelo de avaliação de riscos e altera o "foco" da Auditoria Interna, que em vez de olhar para os processos de negócio como fazendo parte de um sistema de controlo, analisa-os numa perspectiva de risco. Uma auditoria baseada no risco acrescenta mais valor a uma organização do que uma auditoria assente nos controlos, uma vez que os controlos por si só não garantem o sucesso.

A auditoria baseada em riscos, significa ampliar a perspectiva de todas as auditorias internas, quer sejam financeiras, da qualidade, ambiental, da segurança da informação, etc., para abarcar todas as etapas da gestão de risco, incluindo as actividades de controlo (McNamee, 1997b).

De referir que a AIBR, permite ao auditor verificar não só se os controlos existentes são suficientes e eficazes na mitigação dos riscos, mas, também verificar se existem controlos excessivos, podendo recomendar a existência de menos controlos caso se venha a confirmar que os mesmos são ineficazes ou que os custos são demasiado elevados face ao risco.

Neste sentido, espera-se que a Auditoria Interna seja, principalmente, uma ferramenta de apoio à Gestão e que ajude a organização a alcançar os seus objectivos.

De acordo com Cocurullo e Vanca (2002), a avaliação do risco, em auditoria é utilizada para determinar as áreas a auditar com maior prioridade. A avaliação do risco permite ao auditor definir um programa de auditoria capaz de testar os controlos mais importantes ou com maior detalhe.

Conforme referido por Morais (2008), a Auditoria Interna vive um momento único na sua história tornando-se um dos principais alicerces da estrutura de governo das organizações. O papel da Auditoria Interna é mais abrangente, incorpora os processos

de gestão de riscos, auxiliando na prevenção de perdas e na identificação de oportunidades de melhoria dos instrumentos de gestão e controlo das operações.

Para Almeida (2006), a Auditoria Interna contribui para um maior conforto e garantia no controlo dos riscos de negócio; fomenta o alinhamento de objectivos nos vários níveis da organização e é um agente de mudança, já que permite assumir mais risco e aproveitar oportunidades.

De salientar a importância da Auditoria Interna no Governo das Sociedades. De acordo com Câmara (2008:12), "a Auditoria Interna favorece a qualidade da informação financeira, incrementando uma prestação de contas eficiente por parte dos órgãos de administração".

Tendo em consideração as opiniões apresentadas sobre a nova realidade da Auditoria Interna, podemos concluir que todos são unânimes em referir que chegou uma nova era para a Auditoria Interna. A Auditoria Interna deixa de exercer funções meramente de controlo (análise de factos passados), passando a ter uma atitude muito mais pró-activa e de colaboração com a gestão, no que diz respeito à identificação, análise e avaliação dos riscos de negócio (factos presentes e futuros), cujo objectivo é ajudar a Gestão a atingir os objectivos definidos acrescentando, deste modo, valor à organização.

2.2. Controlo Interno

O conceito mais comum de Controlo Interno está relacionado com as normas e procedimentos definidos na organização e que têm como objectivo auxiliar todos os colaboradores na execução das tarefas no âmbito da sua função. Podemos dizer que são um conjunto de regras que definem as melhores práticas a seguir, cujo objectivo final é a salvaguarda dos interesses da empresa.

De referir que inicialmente a Auditoria Interna era baseada nos controlos, o que estava em causa era essencialmente garantir o cumprimento da legislação e regulamentos aplicáveis: normativos contabilísticos, fiscais e sectoriais.

Conforme referido por Gonçalves (2008), foi publicado em 1987 o primeiro documento que trata da temática do Controlo Interno, o denominado Treadway Report[1]. Neste relatório foram, efectuadas uma série de recomendações, nomeadamente para a existência de um Comité de Auditoria composto por profissionais independentes,

[1] Report of the National Commission on Fraudulent Financial Reporting (National Commission on the Fraudulent Financial Reporting, 1987),

competentes e que possuíssem um adequado conhecimento da actividade desenvolvida, bem como, a emissão de relatórios de auditoria que descrevessem a eficácia das medidas de controlo interno.

No seguimento deste relatório (Treadway Report*),* foi desenvolvido e publicado em 1992, pelo COSO, um trabalho sobre o Controlo Interno, designado por "Internal Control-Integrated Framework".

Este documento foi desenvolvido por um grupo de trabalho que Treadway Commission formou com o objectivo de uniformizar o conceito de Controlo Interno, uma vez que existiam várias opiniões sobre este tema, dependendo da pessoa e da função que a mesma desempenhava. Digamos que não havia um entendimento comum, sobre o que é o Controlo Interno e qual a sua missão.

Este grupo de trabalho estava constituído por representantes da American Accounting Association (AAA), American Institute of Certified Public Accountants (AICPA), Financial Executive Institute (FAI), Institute of Internal Auditors (IIA) e Institute of Management Accountants (IMA), e as suas siglas COSO correspondem ao Committee of Sponsoring Organizations of the Treadway Commission,

Este modelo é considerado uma das referências a nível mundial para a auditoria aos controlos internos.

De acordo com o COSO, Controlo Interno é um processo, desenvolvido pelo Conselho de Administração, Órgãos de Gestão e outros elementos da organização definido com o propósito de garantir uma segurança razoável com vista ao cumprimento de metas, atendendo aos seguintes objectivos do controlo:

- garantir a eficácia e eficiência das operações
- garantir a fiabilidade da informação
- assegurar o cumprimento com obrigações legais e regulamentares

Esta definição de Controlo Interno continua a ser aceite em todo o mundo e o objectivo principal, conforme definição acima é de auxiliar a empresa a atingir os seus objectivos.

Pereira et al. (2008) considera que os objectivos referidos nesta definição podem apresentar-se de uma forma mais detalhada, como:

- Salvaguarda dos activos da empresa, prevenção e detecção de fraudes e erros;

- Exactidão, integridade e fiabilidade da informação financeira e contabilística;
- Conformidade com as normas e políticas em vigor na empresa e com as leis e regulamentos aplicáveis.

O Controlo Interno é da responsabilidade de todas as áreas da organização, uma vez que todos trabalham com o mesmo fim, isto é, alcançar os objectivos definidos pela Gestão. No entanto, o Controlo Interno proporciona uma garantia razoável e não uma garantia absoluta de que os objectivos sejam atingidos.

Segundo Gonçalves (2008), o Guia elaborado pelo IFAC para as PME's (Guide to Using International Standards on Auditing in the Audits of Small-and Medium sized Entities") defende que existe uma relação directa entre os objectivos de uma entidade e o sistema de Controlo Interno implementado de modo a garantir a sua realização.

De acordo com Ferreira (2002), o Controlo Interno auxilia a organização a atingir os seus objectivos, mas não garante que os mesmos sejam alcançados, por vários motivos, como por exemplo, o custo/benefício que a implementação de um controlo tem para a organização. Como sabemos, todo o controlo tem um custo, que deve ser inferior à perda que se pode vir a ter caso ocorra o risco.

De acordo com Pereira et al. (2008), os Controlos Internos auxiliam na consecução dos objectivos, mas não garantem que estes sejam atingidos. Isto ocorre segundo o autor devido, principalmente, a três motivos básicos:

- **Custo/benefício**. Todo o controlo tem um custo que deve ser inferior ao custo da concretização do risco que está a ser controlado.
- **Conluio entre pessoas**. As pessoas responsáveis pelos controlos, também podem usar os seus conhecimentos para burlar o sistema com objectivos ilícitos em parceria com outros funcionários, clientes ou fornecedores.
- **Eventos externos**. Eventos externos estão além do controlo de qualquer organização, podendo ser responsáveis por levar um negócio a deixar de alcançar as suas metas operacionais ou até mesmo encerrar as actividades de uma organização.

De acordo com Beja (2004a), o Controlo Interno é um dos componentes que integra os procedimentos específicos da gestão de risco de negócio. Tem como principal função salvaguardar o valor, os interesses e as responsabilidades de uma empresa.

Este conceito tem evoluído de tal modo que hoje em dia, já se relaciona o Controlo Interno com o Risco Empresarial, conforme poderemos verificar no ponto seguinte, em que o COSO passou a integrar componentes de gestão de risco.

Beja (2004a:90) chama a atenção para o facto de se confundir Controlo Interno com Gestão de Risco referindo que "O Controlo Interno é um dos controlos intrínsecos aos procedimentos específicos de gestão de riscos de negócio que, como processo visando salvaguardar o valor, os interesses e as responsabilidades da empresa e minimizar os riscos decorrentes da sua actividade operacional, é por vezes confundido com o Risk Management".

De acordo com Martin e Morales (2001), os sistemas de Controlo Interno e o modo como são aplicados evoluem com o tempo, pelo que os procedimentos que eram eficazes num determinado momento podem perder a sua eficácia ou deixarem de se aplicar. Assim, as empresas têm de verificar e garantir que o actual sistema de Controlo Interno é o adequado e é capaz de detectar os riscos do negócio que estão em constante mutação.

Temos assistido nos últimos anos a uma evolução bastante acentuada dos sistemas de governo das sociedades, sobretudo na resposta dada a falhas e fraudes que surgiram em grandes empresas como a Enron e a WorldCom, nos anos 2001/2002. Estas falhas de controlo ajudaram a perceber como é que é possível acontecerem situações deste tipo, resultando em melhorias no sistema de governo das sociedades, nomeadamente na implementação de novos controlos. Em resposta a estes escândalos corporativos a SEC (Securities and Exchange Commission) implementou novas condições para a gestão e administração das empresas através da Lei Sarbanes-Oxley de 2002 dos Estados Unidos da América, em que obriga as empresas cotadas a apresentarem um relatório anual sobre os seus controlos, o qual, segundo a Secção 404 – Lei Sarbanes-Oxley, 2002: "(1) indicará a responsabilidade da gestão em estabelecer e manter uma estrutura adequada de controlos internos e procedimentos com vista à emissão das demonstrações financeiras; e (2) conterá uma avaliação, à data do termo do mais recente ano fiscal, da Emissora, da eficácia da estrutura dos controlos internos e procedimentos da Emissora para a emissão dos relatórios financeiros" (IPAI, 2002).

É, ainda, referido na secção 404 da Lei Sarbanes-Oxley (IPAI, 2002) relativamente à avaliação dos controlos internos, que cada empresa de auditoria registada que prepare ou emita o relatório de auditoria para a emissora atestará e divulgará a avaliação feita pela gestão da emissora.

Estas disposições, assim como outras semelhantes que têm vindo a ser implementadas neste âmbito, nos diversos países, muito têm contribuído para o desenvolvimento e reforço da importância do controlo interno.

2.3. Principais diferenças entre Controlo Interno e Auditoria Interna

Por força dos seus objectivos o Controlo Interno e a Auditoria Interna andam sempre ligados, no entanto, são conceitos que existem individualmente, isto é, podemos ter Controlo Interno dentro de uma empresa sem que exista Auditoria Interna e a Auditoria Interna não se resume ao acompanhamento do Controlo Interno.

Assim, com o objectivo de clarificar as principais responsabilidades de cada um dos conceitos referidos, Controlo Interno e Auditoria Interna, apresentamos o quadro abaixo:

Controlo Interno	Auditoria Interna
Um processo integrado, ou seja, a definição e controlo é da responsabilidade da Gestão de Topo e Intermédia.	Deve proceder à análise e avaliação do sistema de Controlo Interno instituído na empresa pela Gestão de forma independente.
A Gestão Operacional tem como preocupação manter-se devidamente actualizada.	Embora não seja responsável pela definição do Controlo Interno, deve sempre que possível contribuir para a sua melhoria.
A responsabilidade transmite-se do Topo para a Base.	Deve exercer a sua actividade com carácter regular e utilizar metodologias adequadas.
O reporte da informação deve ser controlado pela estrutura hierárquica definida na empresa	O reporte da informação é efectuado para o Comité de Auditoria, Conselho de Administração, Comissão Executiva e Gestores de Topo, conforme a estrutura organizativa da empresa a auditar.

Quadro 2: Principais diferenças entre CI e AI (**Fonte:** Adaptado de Morais (2000))

Actualmente, de acordo com Martin e Morales (2001), a Auditoria Interna pode e deve contribuir para o cumprimento dos objectivos fixados pela Gestão e, a um nível inferior, aos de cada área ou unidade de negócio da empresa mediante a avaliação dos controlos que contribuem para alcançar esses mesmos objectivos.

2.4. As Normas Internacionais para a Prática Profissional de Auditoria Interna

De acordo com o IIA, as *Normas* estão direccionadas para questões de princípios, e fornecem um enquadramento para o desempenho e promoção de Auditoria Interna. As *Normas* são requisitos obrigatórios e consistem em:

- Declarações de requisitos básicos para a prática profissional de Auditoria Interna e para a avaliação da eficácia do seu desempenho, aplicáveis internacionalmente, a nível individual e da organização.
- Interpretações que clarificam os termos ou os conceitos no âmbito das Declarações.

As normas internacionais para o exercício de Auditoria Interna emitidas pelo IIA (2009) referem-se também ao papel da Auditoria Interna no processo de gestão de risco. Assim, no Quadro 3, apresentamos as normas que consideramos mais relevantes no contexto do nosso trabalho.

Norma de Desempenho	Objectivo da norma
2000 - Gestão da Actividade de Auditoria Interna	"O responsável pela auditoria tem que gerir com eficácia a actividade de Auditoria Interna, de forma a garantir que a mesma acrescenta valor à organização"
2010.A1 - Planeamento	"O responsável pela auditoria tem que estabelecer planos, baseados no risco, para determinar as prioridades da actividade de Auditoria Interna consistentes com os objectivos da organização".
2060 – Reporte aos Gestores de Topo e da Administração	"O responsável pela auditoria tem que relatar periodicamente aos Gestores Superiores e ao Conselho sobre os objectivos, autoridade, responsabilidade e desempenho de Auditoria Interna, relativamente ao seu plano. O reporte tem igualmente que incluir as exposições significativas ao risco e questões de controlo, incluindo riscos de fraude, questões relativas ao governo e outros assuntos necessários ou que tenham sido solicitados pelos gestores superiores e pelo Conselho".

Norma de Desempenho (continuação)	Objectivo da norma (continuação)
2100 – Natureza do Trabalho	"A actividade de Auditoria Interna tem que avaliar e contribuir para a melhoria dos processos de governação, de gestão do risco e de controlo, utilizando uma abordagem sistemática e disciplinada".
2120 – Gestão de riscos	"A actividade de Auditoria Interna tem que avaliar a eficácia e contribuir para a melhoria da gestão do risco".
2600 – Resolução da Aceitação dos Riscos pelos Gestores de Topo	"Quando o responsável pela auditoria for da opinião de que os Gestores de Topo optaram por um nível de risco residual que possa ser inaceitável para a organização, o responsável pela auditoria tem que discutir o assunto com os Gestores de Topo. Caso a decisão sobre o risco residual não tenha sido resolvida, o responsável pela auditoria tem que reportar o assunto à Administração para decisão superior".

Quadro 3: Normas de Desempenho IIA, relevantes na GR (**Fonte:** Produção própria)

Conforme se pode ver no quadro acima, os standards de Auditoria Interna endereçam e incorporam, de forma clara e exaustiva, os riscos no processo de auditoria.

Esta nova visão da Auditoria Interna focada no risco, levou a uma redefinição do papel do Auditor e do trabalho que o mesmo deve desenvolver. Mesmo no que se refere ao papel e abordagem da Auditoria Externa denota-se que a actual redacção das Normas Internacionais de Auditoria emanadas pelo IAASB (International Auditing and Assurance Standards Board) da IFAC, nomeadamente, a ISA 300 (Planear uma Auditoria de Demonstrações Financeiras) e 315 (Identificar e Avaliar os Riscos de Distorção Material por Meio da Compreensão da Entidade e do seu Ambiente), foi claramente influenciada por estes desenvolvimentos.

De acordo com Barros (2006), a actual redacção das normas da IFAC está em linha com a uma nova abordagem do risco de auditoria, que passa, pela consideração do risco de negócio nas avaliações do risco de auditoria. Estando esta visão patente, quanto a nós, nas várias vertentes da auditoria.

3. Gestão de Risco Empresarial

3.1. Evolução e Conceito

De acordo com Beja (2004a), o conceito de Gestão de Risco que representa o conjunto de meios utilizados na identificação, avaliação e relato do risco empresarial, surgiu nos Estados Unidos da América, e foi referido pela primeira vez num artigo publicado no Harvard Business Review no ano de 1956. No entanto, só nos finais do Século XX, é que a Gestão de Risco foi considerada como um elemento importante e essencial no governo empresarial. A Gestão de Risco Empresarial passou a fazer parte das boas práticas de gestão, apoiando a tomada de decisão.

Na mesma linha de pensamento está o Instituto Argentino de Normalização y Certificação (IRAM, 2004) que considera a gestão de risco como parte integrante de uma boa prática de gestão e um elemento essencial no bom governo corporativo.

Um dos nossos maiores empresários referiu a importância crescente da gestão de risco nas empresas na intervenção proferida no Risk Management Forum 2005 da FERMA, afirmando que a gestão de risco envolve um conjunto muito diversificado de actividades e acções, que vão desde as que se relacionam com os riscos dos negócios, até às que dizem respeito aos riscos dos processos operacionais da empresa. Defendendo que, esta gestão deve ser integrada e unificadora, dado que as decisões tomadas por uma determinada área para reduzir os seus riscos poderão criar ou aumentá-los noutra área (Azevedo, 2005).

A Gestão de Risco, de acordo com o Instituto de Gestão de Risco (IRM) de Londres, conforme citado por Willsher (2007:45), “é o processo que pretende ajudar as organizações a compreender, avaliar e actuar sobre todos os seus riscos, para aumentar a probabilidade de sucesso e reduzir a de fracasso”.

De acordo com Azevedo (2005:14) “criar valor implica assumir riscos, conhecê-los e geri-los dá-nos uma força necessária para a fabulosa “aventura” que é de criar riqueza e emprego”.

Segundo o COSO ERM a Gestão de Risco Empresarial é “um processo, desenvolvido pelo Conselho de Administração, Órgãos de Gestão e outros elementos da organização, aplicado na definição da estratégia e que deve abranger toda a organização.

Este processo tem como objectivo a identificação dos eventos que podem afectar a organização e a gestão dos riscos, alinhados com o perfil de exposição definido, com vista a providenciar uma segurança aceitável com vista ao cumprimento dos objectivos definidos pela organização" COSO (2004a:16)[2].

A gestão de risco é um meio para atingir um fim e, não um fim em si mesmo. É um processo educativo que nos consciencializa que de facto existem riscos, e que aos gestores cabe a responsabilidade de os gerir.

De acordo com Castanheira e Rodrigues (2006a) o principal objectivo da gestão é evitar que a empresa sofra as consequências de surpresas desagradáveis.

De acordo com FERMA "a gestão de risco deve ser um processo contínuo e em constante desenvolvimento aplicado à estratégia da organização e à implementação dessa mesma estratégia. Deve analisar metodicamente todos os riscos inerentes às actividades passadas, presentes e, em especial, futuras de uma organização" (FERMA, 2003:3).

De acordo com a nova norma internacional sobre gestão de risco, publicada em Dezembro de 2009, ISO 31000: 2009, e referido por Simões (2009), a gestão de risco consiste num conjunto de actividades coordenadas que visam gerir e controlar os riscos de uma organização.

A tentativa de redução da incerteza é a origem da gestão profissional de riscos, de acordo com Veja (2003). O mesmo autor refere, ainda, que a gestão de riscos, nomeadamente, os operacionais e os de cumprimento, servirá para melhorar o Controlo Interno e, portanto, como medida para potenciar o bom governo corporativo. Nestes últimos anos, a gestão de riscos, de um modo geral, tem procurado aproveitar as oportunidades de ganho e minimizar os impactos negativos. A "nova" gestão de risco é parte integrante das boas práticas de gestão empresarial e é um elemento essencial do governo empresarial.

A gestão de risco é desenvolvida como um processo interactivo, que permite a melhoria contínua da tomada de decisões e do desempenho da organização (Cicco, 2010).

Na gestão de riscos devem ser utilizadas metodologias adequadas, senso comum, conhecimento da cultura organizacional e, ainda, sensibilidade pessoal.

[2] Tradução própria

“A principal diferença entre o processo de ERM e as outras formas tradicionais de gestão de risco é que o processo de ERM adopta uma perspectiva que coordena a gestão de risco ao longo de toda a organização, em vez de cada área da organização gerir os seus próprios riscos” (Banham, 2004) citado por Castanheira e Rodrigues (2006b:58).

Segundo a KPMG (2006:4) o ERM “é uma proposta disciplinada e estruturada que alinha a estratégia, os processos, as pessoas, a tecnologia e o conhecimento, com o objectivo de avaliar e gerir as incertezas que a empresa enfrenta à medida que cria valor”.

3.2. Risco

A noção de risco nem sempre é pacífica, no entanto, está sempre relacionada com os efeitos possíveis da ocorrência de um evento. Em regra, está associado ao efeito negativo dessa ocorrência.

Assim, o risco é a possibilidade de um evento ocorrer e afectar negativamente a concretização de um objectivo planeado, seja por uma pessoa ou por uma empresa.

No mesmo sentido temos Borge (2001), citado por Beja (2004a:81) que considera que “Risco significa estar exposto à possibilidade de um resultado negativo”.

Cicco e Fantazzini (2003) consideram ainda que risco, pode significar por um lado a incerteza quanto à ocorrência de um determinado evento (acidente) e por outro a probabilidade de perda ou perdas que uma empresa pode sofrer em consequência de um ou de vários acidentes.

O COSO define risco como sendo a possibilidade de um evento ocorrer e afectar negativamente a realização dos objectivos. Contudo, os eventos podem resultar de fontes internas ou externas à organização e podem causar impactos positivos e ou impactos negativos. Neste sentido, o COSO refere o seguinte:

> “Os que geram impacto negativo representam riscos que podem impedir a criação de valor ou mesmo destruir o valor existente. Os de impacto positivo podem contrabalançar os de impacto negativo ou podem representar oportunidades, que por sua vez representam a possibilidade de um evento ocorrer e influenciar favoravelmente a realização de objectivos”(COSOa, 2004:28).

Na sequência do impacto poder ser negativo ou positivo encontramos o ideograma chinês que apresenta Risco/Crise através de dois símbolos, conforme figura1.

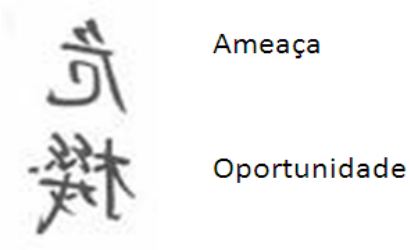


Figura 1: Ideograma Chinês (Risco/Crise) (**Fonte**: Cocurullo, 2008:4)

O ideograma chinês para "Crise/Risco" é a combinação de dois símbolos. Um significa a "Ameaça", o outro pode ser traduzido como "Oportunidade". Apesar da crise, riscos e ameaças, podemos estar diante de uma grande oportunidade de negócio. Por vezes, os riscos tornam-se em oportunidades. Desta forma, curiosamente os chineses na noção de risco tem os dois conceitos associados, ameaça (negativo) e oportunidade (positivo).

No mesmo sentido temos a opinião que abaixo transcrevemos:

> "Quando investidores compram acções, cirurgiões realizam operações, engenheiros projectam pontes, empresários abrem seus negócios e políticos concorrem a cargos electivos, o risco é um parceiro inevitável. Contudo, as suas acções revelam que o risco não precisa ser hoje tão temido: administrá-lo tornou-se sinónimo de desafio e oportunidade". (IBGC, 2007).

De acordo com Hussein (2008), o American Institute of Certified Public Accountants (AICPA), classificou os riscos em três grupos, a saber:

- Riscos relacionados com o ambiente empresarial – ameaças do ambiente empresarial em que a entidade opera, como riscos decorrentes da actuação da concorrência, políticos, legais ou decorrentes da acção de órgãos reguladores e fiscalizadores, financeiros e de procura;
- Riscos relacionados com o processo de negócio e dos seus activos – ameaças ao negócio da organização pelos concorrentes e perdas de activos, sejam físicos ou financeiros; e,

- Riscos relacionados com as informações – ocorrência de ameaças decorrentes de má qualidade das informações para o processo de tomada de decisão e, fornecimento de informações a terceiros.

De acordo com FERMA (2003:3) “o risco pode ser definido como a combinação da probabilidade de um acontecimento e das suas consequências (ISO/IEC Guide 73)”.

De acordo com Beja (2004b) o risco constitui uma componente intrínseca do negócio e a informação sobre os riscos do negócio assume-se como um dos principais temas do moderno governo empresarial.

A nova norma internacional sobre Gestão de Risco, ISO 31000:2009, segundo Simões (2009), define que o Risco “é o efeito da incerteza nos objectivos”.

No mesmo sentido, Morais e Martins (2007), defendem que o risco é importante e interfere no trabalho dos auditores internos, já que a necessidade de controlo é tanto maior quanto maior for o risco.

3.3. Utilizadores da Gestão de Risco

O risco está no centro das atenções de toda a organização, desde o Conselho de Administração, Gestores de Topo, Gestores Operacionais, Auditores e Reguladores Externos, Auditoria Interna e Comité de Auditoria (quando existe), como podemos observar na figura 2. A Auditoria Interna reporta directamente ao Comité de Auditoria, caso a empresa disponha deste órgão, caso, não disponha, deve reportar à Administração. Assim a decisão da Auditoria Interna focar o seu trabalho na identificação e avaliação dos riscos parte de instruções dadas pelo Comité de Auditoria, conforme se apresenta na figura seguinte, ou da Administração. O Série Risk Management (2007) refere que a Auditoria Interna deve obter junto do Comité de Auditoria e da Administração orientações sobre a natureza da garantia objectiva que esperam obter com a actividade da Auditoria Interna, podendo prioritizar os riscos que considerem, mais relevantes.

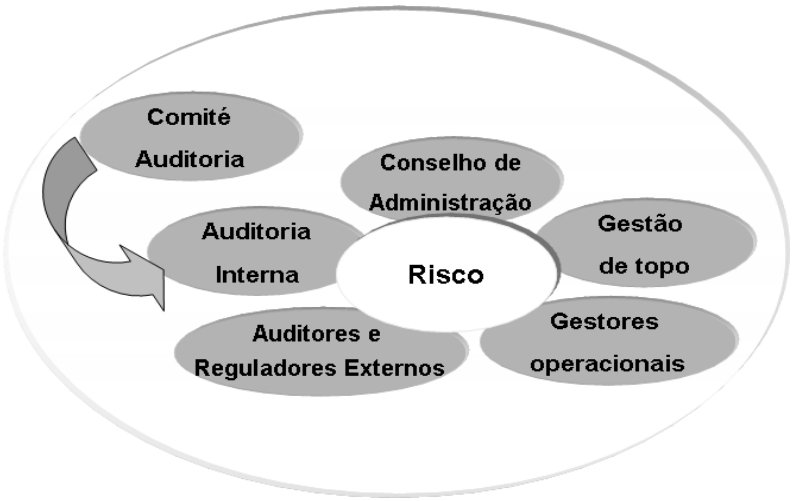


Figura 2: Principais interessados (**Fonte**: Produção própria)

Neste sentido, o Série Risk Management (2005:8:) refere o seguinte:

> "A gestão de riscos motiva a organização a identificar interna e externamente as partes envolvidas e a desenvolver um diálogo de mão dupla entre elas e a organização"

3.4. Modelos de Gestão de Risco Empresarial

Existem vários modelos de gestão de risco empresarial. Contudo, vamo-nos focar naqueles que consideramos mais relevantes, nomeadamente o COSO ERM, a norma AS/NZS 4360:2004, a Norma de gestão de risco – Ferma, o COBIT e faremos uma pequena abordagem à última norma emitida sobre o tema, a ISO 31000:2009.

3.4.1. O COSO ERM

Em 2001, o COSO iniciou um projecto, em parceria com a PricewaterhouseCoopers com vista ao desenvolvimento de um modelo que permitisse ajudar os gestores na avaliação e melhoria da gestão de risco das suas organizações.

Nos últimos anos, os escândalos financeiros das empresas que manipularam as informações financeiras como a Enron, Tyco, WorldCom e outras, afectaram de forma significativa a confiança dos investidores, funcionários e outros "stakeholders", vindo reforçar a necessidade de maior transparência e fiabilidade na realização e divulgação de informação contabilística e financeira e introdução de medidas de melhoria e

reforço de competências ao nível da governação corporativa e da gestão de risco, através de novas leis e regulamentações.

Estes factos vieram reforçar a necessidade do desenvolvimento de um modelo de gestão de risco que fornecesse princípios e conceitos chave, uma linguagem comum e que constituísse um guia para a Gestão de Risco nas organizações.

O modelo de Gestão de Risco (publicado em Setembro de 2004), designado Gestão de Riscos Corporativos – Estrutura Integrada, emitido pelo Committee of Sponsoring Organizations of the Treadway Commission (COSO) com a colaboração da PriceWaterHouseCoopers expande-se para além do sistema de Controlo Interno, promovendo uma focalização mais forte e abrangente na gestão de risco empresarial.

Não substitui o modelo de controlo interno desenvolvido pelo COSO em 1992, mas incorpora-o, permitindo que as organizações adoptem este modelo com vista a satisfazerem as necessidades do seu sistema de controlo interno, progredindo para um processo de gestão de risco.

O COSO - Gestão de Riscos Corporativos – Gestão Integrada, inclui também outra categoria de objectivos, denominados objectivos estratégicos, que operam a um nível superior dos outros objectivos que resultam da missão ou visão da entidade, com as quais deveriam estar alinhados os objectivos operacionais, de informação e de cumprimento, bem como, inclui o conceito de apetite ao risco e tolerância ao risco.

De salientar que todos os dias, as organizações enfrentam incertezas, desafios e uma diversidade de riscos, sendo o grande desafio da Gestão determinar qual é o nível de incerteza para o qual a empresa está preparada para aceitar. Nem todos os riscos apresentam o mesmo nível de importância. A gestão de riscos corporativos permite aos gestores identificar, avaliar e gerir os riscos de acordo com as incertezas, focando-se nos riscos cujo impacto seja maior – quer seja positivo quer seja negativo, com o objectivo de criar valor para os accionistas.

O modelo de Gestão de Risco proposto pelo COSO-ERM é apresentado como um modelo de referência, não só a nível internacional como também a nível nacional.

O modelo de gestão de risco proposto pelo COSO-ERM está assente em 8 componentes que são afectados de acordo com os objectivos da organização. Estes objectivos podem ser classificados em: Estratégicos, Tácticos, Comunicação, Regulação e Conformidade Legal.

Existe uma relação directa entre objectivos e componentes, uma vez que os objectivos são metas que a entidade pretende alcançar e os componentes são os meios necessários para atingir esses objectivos.

Esta relação é representada através de uma matriz tridimensional, com o aspecto de um cubo, conforme figura a seguir:

Figura 3: Cubo do COSO ERM (**Fonte**: COSO, 2004b)

O modelo deverá ser avaliado e implementado de uma forma abrangente a toda a organização, partindo de um nível mais elevado (Entidade) até chegar ao nível mais básico (Actividades).

De acordo com este modelo, os componentes da gestão do risco estão identificados como sendo os seguintes:

Ambiente Interno, ou seja**,** contexto ou ambiente onde as organizações funcionam com objectivos a atingir e meios a serem utilizados para esse fim. Abrange a cultura da organização, a base como o risco é visto e dirigido por uma entidade, incluindo a gestão do risco, a consciência interna sobre risco, a integridade, os valores éticos e o ambiente em que a empresa opera.

Definição de Objectivos, é uma pré-condição para a identificação dos riscos, para a sua avaliação e formulação das respostas possíveis de serem implementadas.

Identificação de Eventos/Acontecimentos, trata-se de identificar os factores internos e externos, com capacidade de influenciar a estratégia e os seus objectivos. Os factores externos compreendem a conjuntura económica/financeira, factores sociais, políticos, tecnológicos e de natureza ambiental. Os factores internos estão ligados às

infra-estruturas, aos activos humanos, aos processos de trabalho e à tecnologia aplicada.

Avaliação dos Riscos, a gestão avalia a situação potencial subdividindo o conceito de risco em risco inerente (aquele em que a organização incorre na ausência de medidas preventivas ou de correcção) e risco residual (risco que permanece mesmo depois de tomadas as acções preventivas e/ou correctivas de comportamentos). Os riscos são valorizados mediante a probabilidade de ocorrência do acontecimento e das suas consequências ou impactos.

Na análise dos riscos, pode-se recorrer a análises qualitativas ou quantitativas dos mesmos. A análise qualitativa faz a prioritização dos riscos através da avaliação e combinação da probabilidade de ocorrência e impacto. Já a análise quantitativa faz a análise numérica do efeito dos riscos identificados nos objectivos gerais.

Resposta aos Riscos, isto é, depois de identificados e avaliados os riscos, a gestão deve preparar respostas que obedecem inevitavelmente às seguintes possibilidades: evitar o risco, reduzir o risco, partilhar o risco ou aceitar o risco.

A resposta ao risco é o processo de desenvolver e determinar acções para mitigar os riscos, reduzindo as ameaças dos objectivos da organização. A administração avalia a probabilidade e o impacto da ocorrência do risco, os custos e benefícios, a prioridade das acções a implementar e selecciona a resposta que melhor se adequar dentro dos limites de tolerância do risco aceite.

Controlo das actividades, este controlo deve ser efectuado através do vector risco. Como tal deve ser enquadrado/identificado com as políticas (o que deve ser feito) e os procedimentos (a forma como se deve fazer) que garantem a resposta aos riscos.

Informação e comunicação, torna-se particularmente importante, com vista a facilitar a criação de valor acrescentado, formalizar na organização um sistema de informação estratégico.

Monitorização, pode revestir-se de duas formas. A primeira, prende-se com o conhecimento (em tempo real) do desenvolvimento das actividades, sendo a monitorização, neste caso, parte integrante das actividades operacionais definidas numa organização. A segunda consiste em actividades de avaliação, que o departamento de Auditoria Interna e outras entidades desenvolvem, em função do perfil e frequência dos riscos, da dificuldade ou importância das respostas aos riscos e dos seus controlos de gestão.

3.4.2. Norma Australiana / Neozelandesa AS/ NZS 4360:2004

Esta norma fornece orientações genéricas para a aplicação de uma gestão de riscos, podendo ser aplicada em diferentes organizações, quer sejam privadas, públicas ou comunitárias.

O principal objectivo desta norma é o de fornecer orientações às diferentes organizações de modo a que possam ter uma base segura na tomada das suas decisões e na realização do planeamento. Permite identificar oportunidades e ameaças, tirar proveito das incertezas, utilizar de forma mais eficiente os recursos disponíveis, reduzindo perdas e custos, bem como, permite melhorar a segurança e confiança de todos os interessados, melhorar a conformidade com a legislação aplicável e o governo corporativo.

Apresentamos na figura a seguir o modelo de gestão de risco definido na norma Australiana/neozelandesa (AS/NZS 4360:2004). Aliás conforme referimos, utilizamos este modelo de gestão de risco na aplicação prática apresentado neste trabalho.

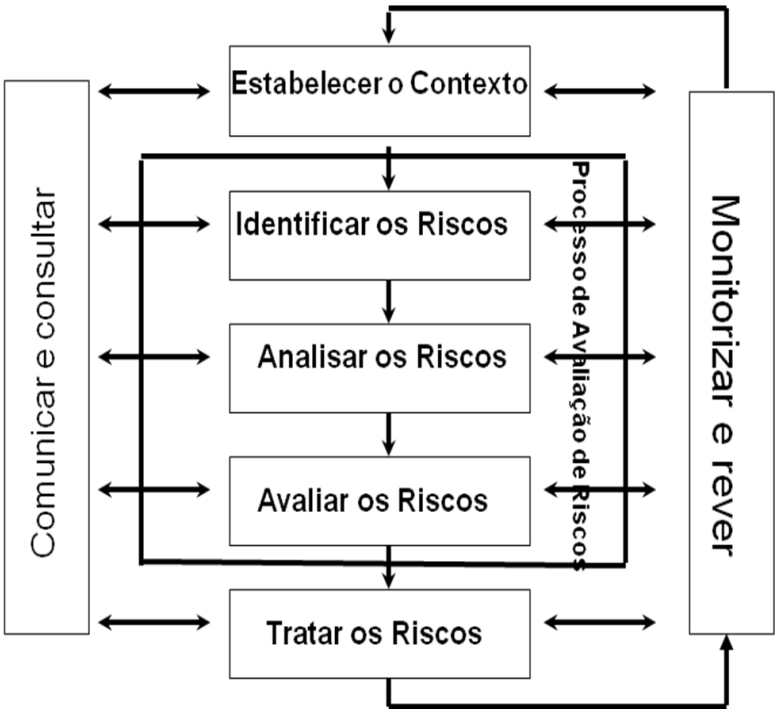


Figura 4: Processo de Gestão de Risco (**Fonte**: AS/NZS 4360:2004:9)[3]

[3] Tradução própria

Apresentamos de seguida uma breve descrição de cada uma das fases deste modelo, tendo por base o esquema acima apresentado, onde se evidenciam os principais elementos do processo de gestão de risco, a própria norma (Série Risk Management; 2004) e as Directrizes para a implementação desta norma (Série Risk Management; 2005).

Em termos gerais, o processo apresenta sete fases devidamente identificadas, a saber: Comunicação e Consulta; Estabelecer o Contexto; Identificar os Riscos, Analisar os Riscos, Avaliar dos Riscos; Tratamento dos Riscos; Monitorizar e Rever.

A fase da Comunicação e Consulta, está associada a todas as fases do processo de gestão de risco e ao processo como um todo. Deste modo, assume uma importância fundamental, já que, é essencial uma comunicação interna e externa eficaz, para garantir que os responsáveis pela implementação da gestão de risco, bem como todos os intervenientes no processo, compreendam a base sobre a qual as decisões são tomadas e porque razão é necessário implementar determinadas acções.

No que diz respeito ao **Estabelecimento dos Contextos**, a norma refere que nesta fase se definem os parâmetros básicos nos quais os riscos devem ser geridos, e define o enquadramento do restante processo de gestão de risco. De salientar a importância do ambiente organizacional e do ambiente externo, no estabelecimento dos objectivos definidos no processo de gestão de risco.

Nesta fase são definidos os contextos externos, internos, da gestão de risco, bem como, o desenvolvimento de critérios e definição da estrutura.

Como exemplo de ambiente externo da organização, temos o ambiente empresarial, social, regulamentar, cultural, financeiro, entre outros. Identificam-se os pontos fortes e fracos da organização e as partes externas envolvidas no processo, bem como, não se pode deixar de ter em consideração as ameaças e oportunidades que surgem do exterior.

O estabelecimento do contexto interno é igualmente muito importante, uma vez que, em qualquer fase é necessário compreender e conhecer muito bem a organização, nomeadamente no que diz respeito à cultura, áreas envolvidas, estrutura organizacional, processos, objectivos definidos e estratégias utilizadas para os atingir.

O estabelecimento do contexto da gestão de riscos, envolve a definição do processo, actividade e objectivos a atingir na aplicação do processo de gestão de riscos. Deve ser definido o âmbito da actividade quer em termos de prazo quer no que respeita à profundidade e extensão das actividades de gestão de risco a serem executadas.

Também podem ser definidas as áreas da organização e responsabilidades das pessoas intervenientes no processo de gestão de risco a implementar.

No início do processo devem ser determinados os critérios de risco apropriados em relação aos quais os riscos serão avaliados e as decisões serão tomadas, nomeadamente no que respeita ao tratamento dos riscos. Os critérios podem ser operacionais, técnicos, financeiros, legais, ambientais, entre outros e, regra geral, dependem das políticas internas, objectivos da organização e dos interesses das partes envolvidas.

Por último, temos a definição da estrutura para o restante processo e que consiste em subdividir a actividade ou, processo em conjuntos de etapas, de modo a garantir que todos os riscos importantes são identificados. A estrutura escolhida depende da natureza dos riscos e da estrutura do processo ou actividade.

A fase que se segue á a da **Identificação dos Riscos**, cujo objectivo é identificar os riscos que devem ser geridos. É importante que nesta fase sejamos muito cuidadosos, de modo, a evitar falhas na identificação de riscos, quer estejam sob controlo ou não da organização, isto porque, uma falha nesta fase poderá implicar que esses riscos não sejam identificados nas fases posteriores.

Nesta fase, vamos procurar dar resposta a quatro perguntas: o que pode acontecer, onde, quando e como? Vamos tentar identificar todos os eventos possíveis que possam de algum modo afectar positiva ou negativamente a concretização de objectivos do processo em análise. Cada evento pode ocorrer de várias maneiras pelo que é importante que não nos esqueçamos de nenhuma causa possível.

As ferramentas e técnicas utilizadas na identificação dos riscos incluem checklists, observações e opiniões suportadas no conhecimento da organização e dos processos em análise, fluxogramas e descritivos de actividades e processos, análise de cenários e de sistemas e entrevistas aos responsáveis e colaboradores da área auditada. De salientar que a escolha das ferramentas e técnicas a utilizar dependem da natureza dos processos em análise, da sua contextualização na organização e do objectivo do trabalho sobre gestão de riscos em causa.

Depois de identificados todos os riscos do processo/sub-processo/actividade, dependendo do detalhe e profundidade do trabalho a executar sobre gestão de riscos, devemos proceder à fase da **Análise dos Riscos**, ou seja, vamos tentar compreender quais os níveis dos riscos identificados, de modo a que nos seja possível decidir qual o tratamento mais adequado para cada um dos riscos, tendo em

consideração a relação custo/benefício da opção tomada. Os níveis dos riscos são determinados através da combinação de dois factores, a Probabilidade e o Impacto. As escalas e técnicas utilizadas para esta combinação dependem dos critérios previamente definidos na fase dos contextos, uma vez que depende muito da situação em análise, dos objectivos e dos recursos disponíveis. A análise pode ser qualitativa, semi-quantitativa, quantitativa e de sensibilidade. Uma análise diz-se qualitativa quando utiliza a descrição em vez de meios numéricos para definir o nível de risco. No método semi-quantitativo, os resultados não podem ser interpretados, uma vez que, não são precisos, contrariamente ao método quantitativo, em que os resultados determinam o nível de risco, uma vez que, foi possível quantificar com algum rigor a probabilidade de ocorrência de um determinado risco e o impacto desse mesmo risco caso venha a acontecer. De referir que nesta fase são identificados os controlos existentes.

A fase seguinte é a **Avaliação dos Riscos**, cuja finalidade é a tomada de decisão, nomeadamente no que diz respeito ao tratamento dos riscos, isto é, a avaliação dos riscos permite-nos catalogar os riscos em função do seu grau de criticidade e prioritização das medidas a tomar e riscos a tratar.

Passamos de seguida para a fase do **Tratamento dos Riscos**, em que se identificam as possíveis opções para tratar os riscos, se analisam e avaliam essas mesmas opções, elaborando-se e implementando-se os planos de acção que se entenderem mais adequados e eficazes, não esquecendo a análise da relação custo/benefício das medidas propostas e se estamos perante riscos com resultado positivo (oportunidades) ou negativo (ameaças).

Conforme referimos acima, são várias as estratégias de gestão de risco que podem ser utilizadas, por exemplo no caso de resultados negativos, podemos optar por evitar o risco (aversão aos riscos), deixando de realizar a actividade que gera esse mesmo risco, ou podemos compartilhar o risco com uma entidade terceira, como por exemplo através do pagamento de um prémio de seguro. Os riscos podem ser partilhados total ou parcialmente. De salientar que quando se decide partilhar o risco, estamos a adquirir um novo risco, uma vez que não há segurança absoluta de que a entidade para quem estamos a transferir o risco, o vai gerir eficazmente. Podemos ainda, optar por reduzir quer a probabilidade de ocorrer quer o seu impacto através da implementação de medidas que mitiguem esses riscos.

Quando estamos perante resultados positivos, as opções para o tratamento deste tipo de riscos, dependem dos objectivos da organização. No entanto, podemos

enumerar possíveis soluções, nomeadamente alterar a probabilidade da oportunidade ocorrer, aumentando a probabilidade dos ganhos que podem resultar deste risco. Também se pode partilhar o risco com uma entidade terceira, como por exemplo através do fornecimento de recursos adicionais que aumentem a probabilidade da oportunidade ocorrer e consequentemente um aumento de resultados positivos.

A última fase deste processo de gestão de risco é **Monitorizar e Rever**, que tem como principal objectivo verificar a evolução real da situação face às recomendações e planos de acção propostos com vista à mitigação e ou redução do nível de risco. Por outro lado, também tem como finalidade analisar e avaliar possíveis alterações no processo que tenham implicação directa ou indirecta na probabilidade ou impacto de um determinado risco acontecer, quer seja um risco já identificado anteriormente, quer seja um risco novo que seja identificado nesta fase.

Embora, não evidenciado neste fluxograma da figura 4, a norma refere que cada etapa de gestão de riscos deve estar devidamente registada e documentada. Aliás trata-se de uma boa prática de Governação Corporativa, para além de um requisito básico de auditoria – recolha e documentação da prova.

3.4.3. Norma de Gestão de Riscos - FERMA

A norma de gestão de riscos da FERMA (2003) é resultado do trabalho de uma equipa composta por elementos das principais organizações de gestão de risco do Reino Unido – The Institute of Risk Management (IRM), The Association of Insurance and Risk Managers (AIRMIC) e The Nacional Forum for Risk Management in the Public Sector (ALARM), cujo objectivo era chegar a um consenso sobre gestão de riscos, uma vez que existem diversos pontos de vista sobre este tema. As normas servem para garantir concordância em relação à terminologia utilizada (esta norma utilizou sempre que possível a terminologia para o risco definida pela Organização Internacional de Normalização (ISO), processo de implementação de gestão de riscos, estrutura organizacional para a gestão de riscos e objectivos da gestão de riscos.

De acordo com esta norma a gestão de riscos é “o processo através do qual as organizações analisam metodicamente os riscos inerentes às respectivas actividades, com o objectivo de atingirem uma vantagem sustentada em cada actividade individual e no conjunto de todas as actividades” (FERMA, 2003:3).

A gestão de riscos deve ser um processo contínuo e em constante desenvolvimento, deve ser integrada na cultura da organização e deve traduzir a estratégia em

objectivos tácticos e operacionais. Toda a organização tem responsabilidades na gestão de riscos.

Esta norma apresenta um processo de gestão de risco. O processo inicia-se com os objectivos estratégicos da organização, partindo-se depois para a fase da avaliação do risco. Esta fase é composta pela análise do risco e pela comparação do risco. A análise do risco engloba a identificação dos riscos ou seja identificar a exposição de uma organização ao elemento incerteza, o que exige um conhecimento bastante aprofundado da organização, a descrição do risco, ou seja, a apresentação dos riscos de forma estruturada e a avaliação do risco, que pode ser quantitativa, semi-quantitativa em termos de probabilidade de ocorrência e possível consequência.

A comparação dos riscos é efectuada quando o processo de análise está concluído, uma vez que se tem de comparar os riscos estimados com os critérios de riscos definidos pela organização e que podem ser exigências legais, factores socioeconómicos e ambientais entre outros.

A fase seguinte corresponde ao reporte do risco, quer se trate de ameaças ou de oportunidades. Depois passa-se à fase da decisão sobre a importância dos riscos para a organização e sobre a possibilidade de cada risco específico ser aceite ou corrigido. Passando-se á fase do tratamento de riscos, ou seja, é o processo de selecção e implementação de medidas para modificar um determinado risco. Esta norma define como elemento principal de tratamento de riscos o controlo/diminuição dos riscos, como por exemplo evitar riscos ou transferi-los (seguros). Por fim, vem o reporte do risco residual, ou seja, a comunicação de riscos dentro da organização a diferentes níveis (Conselho de Administração, Unidades de negócio, Colaborador). Contudo, também pode existir comunicação externa aos seus intervenientes, uma vez que, cada vez mais, se pretende que as organizações apresentem provas de uma gestão eficaz. Por fim, é feita a monitorização de modo a assegurar que os riscos são identificados e avaliados de forma eficaz e que os controlos e as respostas são adequados e eficazes na mitigação dos riscos e que os procedimentos são compreendidos e seguidos.

Em anexo à norma são apresentados exemplos de técnicas de identificação de riscos e de métodos e técnicas de análise de riscos.

3.4.4. O COBIT

Existem dois *modelos* de referência a nível mundial, o modelo publicado pelo COSO para a gestão de riscos dos negócios que analisámos no ponto 3.4.1 e o COBIT

(Control Objectives for Information and related Technology) para a gestão de riscos dos sistemas de informação.

Segundo BLOEM et al. (2005), citado por Sandonato (2007), a prevalência destes modelos decorre da indicação da SEC (Securities and Exchange Commission), responsável pela implantação da SOX, pelo uso de um *Framework* reconhecido, recomendando a implementação de um processo de gestão de riscos, com métodos estruturados de controlos internos que permita alcançar os objectivos de negócio, e refere o modelo COSO como a estrutura de controlos mais recomendada para a conformidade com a SOX.

O COBIT é considerado uma das estruturas mais adequadas para a gestão de TI, e aquela que melhor articula o modelo COSO com a gestão de TI e com o governo das sociedades. O Cobit (2007), refere que existem várias vantagens para implementar este modelo como referência de gestão de TI, nomeadamente, o entendimento entre todos os interessados, através da utilização de uma linguagem comum e o cumprimento dos requisitos definidos pelo COSO, no que diz respeito ao ambiente de controlo de TI.

Os objectivos de controlo detalhados no Cobit relacionam-se com as cinco componentes do controlo interno do COSO.

Assim, como o COSO é o mais indicado e é uma referência mundial no que diz respeito aos controlos internos dos processos de negócios, o COBIT é o mais utilizado para implementar uma estrutura de controlos internos sobre a gestão dos recursos de tecnologias da informação.

Os mapas de controlo fornecidos pelo Cobit auxiliam os auditores e gestores a manter os controlos necessários de modo a garantir os objectivos da organização, através de uma gestão eficaz da informação.

“O COBIT permite o desenvolvimento de políticas claras e de boas práticas para controlar as TI através das empresas” (Cobit 4.1, 2007:8).

O COBIT surgiu a partir de estudos da ISACA – Information Systems Audit and Control Association, *que* foi criada em 1967, com o objectivo de estabelecer, de modo centralizado, uma fonte de divulgação de informações e orientações para os profissionais envolvidos em auditoria de sistemas de informação. O Cobit recebe várias contribuições de empresas e organismos internacionais, nomeadamente Códigos de conduta emitidos pelo ISACA, padrões profissionais para controlo interno e auditoria como por exemplo do COSO, IFAC, AICPA entre outros.

Em 1998, a ISACA criou o ITGI, com o objectivo de alargar os benefícios da aplicação de modelos de governação corporativa na gestão dos recursos de TI.

O COBIT ajuda a gestão a alcançar os seus objectivos quer nos requisitos de eficácia, eficiência e economia, quer no que diz respeito à confidencialidade dos dados, integridade, disponibilidade, conformidade e fiabilidade da informação necessária para controlo e tomada de decisão pela organização.

De acordo com Cobit (2007) a gestão de TI facilita que a empresa aproveite ao máximo a sua informação, maximizando assim os benefícios, aumentando as oportunidades e as vantagens competitivas.

O Cobit está orientado para o negócio, proporcionando a informação necessária para que a empresa atinja os seus objectivos, gerindo e controlando os recursos de TI.

3.4.5. ISO 31000:2009

A ISO 31000:2009, é a mais recente norma mundial lançada sobre gestão de riscos, que fornece princípios e directrizes para a implementação eficaz da gestão de riscos nas organizações, encontrando-se alinhada com a visão integrada da gestão de risco empresarial (ERM).

De acordo com Bastos (2009), o processo de criação da ISO 31000 iniciou-se com a primeira reunião que foi efectuada em Tóquio no Japão em 2005.

Conforme referido por Júnior (2009), a ideia partiu de uma norma australiana que abordava o que deveria ser feito para melhorar a gestão de risco nas empresas.

Passados cerca de cinco anos de trabalho e depois de muitas reuniões, análises e discussões em vários países e com vários especialistas de diferentes sectores de actividade, foi publicada em Novembro de 2009, a tão esperada norma, ISO 31000:2009, com recomendações das melhores práticas em gestão de risco.

De acordo com Bastos (2009), o trabalho demorou a ser concluído por se tratar de uma abordagem que abrange diferentes áreas. Basto (2009) refere ainda que o mais difícil foi conseguir conciliar diferentes áreas e termos utilizados na gestão de risco. Aliás uma das grandes dificuldades foi definir *risco*. Foram apresentadas várias definições de risco. Contudo, conseguiram chegar a uma definição comum de risco amplamente aceite em todas as áreas.

A norma pode ser aplicada em qualquer tipo de empresa, mas não é destinada para fins de certificação. Trata-se de uma norma abrangente e que tem como principal objectivo ajudar os responsáveis pelo desenvolvimento da política de gestão de riscos nas organizações a assegurar que os riscos são eficazmente geridos.

Hoje em dia verificamos que cada área das empresas avalia os seus riscos, utilizando os meios que considera mais adequados, não existe uma gestão integrada do risco. Deste modo, esta norma vem ajudar as organizações a desenvolver, programar e melhorar continuamente uma estrutura com a finalidade de integrar o processo de gestão de riscos no governo, na estratégia, na gestão, nos processos e na cultura de toda a organização.

De acordo com Blair (2009) a nova norma internacional tem por base a norma *AS / NZS 4360-2004* e foi ajustada com a entrada de novos membros experientes e especialistas de cerca de 28 países, representando todos os continentes.

De salientar que a norma AS/NZS 4360:2009, foi substituída pela AS/NZS ISO 31000:2009 Gestão de riscos – Princípios e directrizes.

A novidade desta norma é a inclusão de princípios de gestão e da ênfase que é dada ao risco. O risco é definido como o efeito da incerteza sobre os objectivos, e não apenas como um evento. Cada organização tem objectivos estratégicos, tácticos e operacionais para alcançar e para isso vai ter de saber gerir o efeito da incerteza sobre os objectivos.

Actualmente nas organizações, os departamentos agem isoladamente, avaliando os seus riscos, através de diversas ferramentas. Esta norma tem como principal objectivo ajudar as organizações a desenvolverem, programarem e melhorarem de forma contínua uma estrutura com a finalidade de integrar o processo de gestão de riscos no governo, na estratégia e planeamento, na gestão, nos processos de reportar dados e resultados, nas políticas, valores e cultura de toda a organização.

Ao mesmo tempo, está a ser publicado a ISO Guia 73:2009, vocabulário de gestão de risco, que complementa a ISO 31000:2009, fornecendo um conjunto de termos e definições relativas à gestão de risco, de acordo com ISO (2009).

De acordo com Knight (2009) a ISO 31000 é um documento prático que visa auxiliar as organizações a desenvolver e a implementar a sua própria metodologia de gestão de risco. A ISO 31000, é uma referência a nível internacional, pelo que poderá ser utilizada como referência nas organizações que pretendam implementar um modelo de gestão de risco, proporcionando bons princípios de gestão.

De salientar que em Dezembro de 2009 foi publicada uma nova norma internacional a ISO/IEC 31010:2009 - *Gestão de riscos - Técnicas de avaliação de riscos*. A 31010:2009 é uma norma de apoio à ISO 31000:2009 e fornece orientação sobre a selecção e aplicação de técnicas sistemáticas de avaliação de riscos.
A ISO 31000:2009, (QSP; 2010), utiliza o mesmo processo de Gestão de Risco da norma Australiana/neozelandesa (AS/NZS 4360:2004), conforme apresentado na figura 4.

3.5. Limitações da Gestão de Risco Empresarial

A Gestão de Risco Empresarial, qualquer que seja o modelo que se aplique, não garante que os objectivos de uma organização sejam todos atingidos, apenas dá uma segurança razoável de que tais objectivos possam ser alcançados.

Não nos podemos esquecer que o risco pertence ao futuro, logo é um acontecimento que não é possível prever com segurança e muitos deles não dependem da própria organização, são externos à organização, o que os torna ainda mais difíceis de prever.

A gestão de riscos é feita por pessoas, logo, existe a possibilidade de ocorrer um erro humano, como por exemplo uma informação mal entendida pode dar origem a uma decisão ou um juízo de valor menos correcta, podendo afectar a concretização de determinado objectivo.

Por outro lado, e tendo em consideração os dias de hoje, em que os recursos são escassos, as organizações devem ter em consideração os custos/benefícios da implementação de controlos para a mitigação de riscos, ou até mesmo ponderar se é vantajoso para determinada organização implementar um modelo de gestão de risco.

De acordo com o COSO ERM, o conceito de segurança razoável, não quer dizer que a gestão de riscos corporativa vá fracassar frequentemente. Contudo, pode ocorrer um erro, um evento incontrolável ou uma informação falsa. Uma segurança razoável não constitui uma segurança absoluta.

4. Metodologia da Auditoria Focalizada na Gestão de Riscos

4.1. Processo de Auditoria Interna baseado nos Riscos do Negócio

A AIBR é suportada na análise de riscos do negócio e focalizada nas áreas que apresentam riscos de maior grau de criticidade e urgência.

Actualmente a abordagem de Auditoria Interna está muito direccionada para a focalização no risco, daí que Castanheira e Rodrigues (2006 b:11) refira que “a actual orientação da Auditoria Interna aponta para uma abordagem baseada nos principais riscos do negócio, pelo que o planeamento de auditoria deverá estar alinhado com a estratégia da organização e o plano de negócio”.

De acordo com Cicco (2006), a auditoria, identifica, avalia e prioriza os riscos para se focalizar nas áreas mais importantes a auditar. A avaliação de riscos permite ao auditor delinear um programa de auditoria capaz de testar os controlos mais importantes ou com maior nível de profundidade.

A AIBR não se foca exclusivamente nos riscos da área financeira, não se preocupa só com factos passados e em emitir uma opinião sobre a razoabilidade das Demonstrações Financeiras e o adequado cumprimentos das normas, regulamentos e procedimentos de controlo interno da organização. Passou a ter outra preocupação que se trata de analisar, avaliar e controlar os riscos de negócio. Passou a ter uma atitude mais pró-activa, mais comprometida com a Gestão, no cumprimentos dos objectivos.

Conforme referido pela FERMA (2003), a função da Auditoria Interna é diferente em cada organização. Contudo, na prática, a função de Auditoria Interna pode incluir alguns ou todos os seguintes pontos:

- Focar o seu trabalho nos principais riscos do negócio, identificados pela gestão da organização e efectuar auditorias aos processos de gestão de riscos implementados;
- Garantir que a gestão de riscos é eficaz e apoiar no processo de gestão de riscos da organização;

- Possibilitar a identificação/avaliação de riscos e promover formação sobre gestão de riscos e controlo interno aos colaboradores;
- Gerir a comunicação de riscos que é efectuada ao Conselho de Administração, ao Comité de Auditoria, etc.

De acordo com Cicco (2006) a AIBR começa e acaba com a consideração dos riscos do negócio. Os controlos internos são uma parte importante do tratamento de riscos, mas não são a solução completa.

4.2. Principais Objectivos de uma AIBR

A AIBR tem como principais objectivos fornecer uma segurança razoável no que diz respeito a se:

- os Processos de Gestão de Risco que a gestão implementou na Organização estão a funcionar correctamente, conforme foram definidos e se são adequados;
- as respostas aos riscos são eficazes e adequadas na gestão do risco inerente, reduzindo esses riscos para níveis aceitáveis pela organização;
- estão definidos e correctamente implementados controlos que mitiguem eficazmente os riscos de modo a não colocar em causa a concretização dos objectivos definidos pela gestão;
- os processos de gestão de risco são acompanhados pela gestão de modo a garantir que os riscos, respostas e acções desenvolvidas são eficazes e estão em linha com os objectivos da organização.

Assim, a Auditoria Interna pode dar um apoio importante à gestão na medida em que garante que os processos de gestão de risco são adequados e funcionam de forma eficaz, bem como, garantem a eficácia dos controlos ou identificam necessidades de melhoria dos controlos existentes ou ainda implementação de novas medidas, caso se justifiquem. A Auditoria Interna também garante uma correcta identificação e avaliação dos riscos na organização.

A AIBR tem como principal objectivo determinar quais os objectivos primários do negócio da organização, os riscos associados, o apetite ao risco e níveis de tolerância, de modo a avaliar o grau de eficácia das actividades de gestão do risco empresarial desenvolvidas de forma a garantir a prossecução dos objectivos da organização,

nomeadamente no que diz respeito ás medidas de controlos implementadas e a eficácia das mesmas na redução dos riscos para níveis aceitáveis, de modo a garantir a concretização dos seus objectivos. Estamos perante uma nova abordagem, que visa alinhar os objectivos estratégicos, com os mecanismos de identificação dos riscos, sua avaliação, gestão e acompanhamento efectuado pelos Auditores Internos, conforme referido por Gonçalves (2008).

De acordo com Sumners (1999), a Auditoria Interna tem que se integrar no processo de gestão de risco. Não obstante o facto da organização poder nomear um responsável pela Gestão de Risco, é necessário que os Auditores Internos desenvolvam uma metodologia de avaliação dos riscos do negócio, com a devida independência.

4.3 Razões para a implementação de uma AIBR

Existem várias razões que levam à implementação da gestão de risco numa organização, das quais destacamos o alinhamento e a integração de diferentes visões da gestão de risco, a construção de uma base de confiança em relação aos diferentes parceiros de negócio, o fortalecimento do governo das sociedades, resposta eficaz a eventuais mudanças que possam ocorrer no negócio e o alinhamento da estratégia com a cultura da organização.

A organização ao avaliar os riscos percebe até que ponto os eventos previstos e não previstos podem ter influência no cumprimento dos seus objectivos, bem como avalia qual a probabilidade de tais eventos acontecerem ou não e que impactos podem ter na organização.

A finalidade da análise e gestão do risco de negócio é essencialmente para aumentar a probabilidade e o impacto dos eventos positivos e diminuir a probabilidade e impactos dos eventos negativos.

De acordo com Zárate (2001), e numa perspectiva de evolução da função, a gestão de riscos permite orientar a actividade da Auditoria Interna para as áreas onde se identificaram os riscos mais relevantes do negócio e ou processo, bem como se traduz numa ferramenta extraordinária, uma vez que os Auditores Internos ao focarem o seu trabalho sobre áreas críticas estão em condições de dar uma opinião sobre a razoabilidade da realização de determinados objectivos.

Cada organização deve determinar o modo como quer implementar a gestão de riscos. De salientar que nem todas as empresas estão no mesmo grau de maturidade da gestão de riscos, ou seja, é necessário verificar se já existe uma cultura de gestão de risco formalizada no seio da organização, se existem estratégias e políticas implementadas e comunicadas a todas as áreas da empresa ou se não foi desenvolvida qualquer abordagem sobre gestão de risco. Estes factores são relevantes na implementação de uma AIBR e de acordo com Série Risk Técnologia (2007), a primeira fase da AIBR é analisar de forma critica o nível de maturidade de riscos. Esta obra refere ainda que a Auditoria Interna pode ajudar a melhorar os processos de gestão de riscos e de governo, comunicando os resultados da avaliação sobre a maturidade dos riscos da organização ao Comité de Auditoria e, promovendo a gestão de riscos em todos os trabalhos realizados pela Auditoria Interna.

Uma característica importante da AIBR é que a prioritização é sempre feita tendo em consideração a criticidade dos riscos e a avaliação dos controlos na mitigação desses mesmos riscos.

De acordo com Série Risk Management (2007), seguindo a AIBR, a Auditoria Interna deve poder concluir que a Gestão identificou, avaliou e deu respostas eficazes aos riscos, de modo a alinhar os riscos residuais dentro do apetite ao risco aceite pela organização. A gestão deve garantir que quer os processos de gestão de risco quer a eficácia das respostas e conclusões das acções tomadas pela organização estão a ser monitorizadas e consequentemente continuam a operar eficazmente.

Isto permite que a Auditoria Interna dê ao Comité de Auditoria e à Gestão garantia de que os processos de gestão de riscos são adequados à organização e eficazes na mitigação de riscos, nomeadamente no que diz respeito à eficácia dos controlos implementados, de modo a que não sejam colocados em causa a concretização dos objectivos e metas definidos.

4.4. O Papel do Auditor Interno na Gestão de Riscos

A Auditoria Interna tem um papel importante na avaliação da eficácia da gestão de risco na organização. Deve avaliar com regularidade a eficácia dos controlos internos relativos à quantificação, informação e limitação dos riscos. A avaliação dos diferentes riscos ajudam a Auditoria Interna a definir o seu plano de trabalho, uma vez que lhe permite determinar quais são as áreas de maior risco, isto é, as áreas prioritárias e

sobre as quais devem recair todas as atenções, portanto, as que devem ser analisadas primeiro.

Segundo o COSO (2004a), a avaliação de riscos é uma responsabilidade da Administração, mas cabe à Auditoria Interna fazer uma avaliação própria dos riscos, confrontando-a com a avaliação feita pelos administradores.

De acordo com Cicco (2006), a identificação e avaliação dos riscos nos trabalhos realizados pela auditoria permite identificar quais as áreas mais importantes da organização e consequentemente elaborar um programa de auditoria que permita testar os controlos mais importantes ou com maior detalhe.

Assistimos a uma mudança nos focos da auditoria, ou seja, deixou de se preocupar só com a análise de avaliação de controlos, para se preocupar também com a análise e avaliação do risco (financeiro, operacional, etc.), deste modo a Auditoria Interna gera mais valor para a empresa.

Poder-se-á perguntar se a gestão de risco não extravasa o papel da Auditoria Interna. E a resposta será não. Pelo contrário, até é consistente com as actividades previstas pelo Institute of Internal Auditors (IIA[4], 2004), no que concerne a actividades de segurança e consultoria, modernamente preconizadas. Com a ressalva, que as empresas devem compreender de uma forma integral que a Administração é a responsável pela gestão de risco. Os Auditores Internos devem providenciar conselho e apoiar ou contestar as decisões tomadas pela gestão sobre risco em vez de tomar decisões sobre gestão de riscos. Deste modo, de acordo com o IIA, a Auditoria Interna no âmbito do ERM deve (IIA:2004):

- Certificar os processos de gestão de risco.
- Certificar que os riscos estão correctamente identificados e avaliados.
- Avaliar os processos de gestão de risco.
- Avaliar o reporte dos principais riscos.
- Rever a gestão dos principais riscos.

O IIA (2004), estabelece ainda quais as actividades que a auditoria não deve realizar, por deverem ser da responsabilidade da gestão e quando tomadas pela Auditoria Interna vão diminuir a independência desta nas competências que o IIA lhe atribui. Assim, algumas das actividades que não devem ser realizadas pelo Auditor Interno, são as seguintes:

- estabelecer o apetite ao risco
- estabelecer processos de gestão de risco
- tomar decisões quanto ás respostas a dar aos riscos identificados
- implementar medidas que mitiguem os riscos
- ser responsável pela gestão de riscos.

Neste contexto, para que o Auditor Interno possa desempenhar adequadamente o seu papel é necessário que domine várias matérias. Daí que tenhamos autores como, Sumners (1999:92) que referem que:

> "Os auditores terão que ser primeiro bons Homens de negócio e, em Segundo lugar bons Auditores. Deverão ser conscientes do que passa fora da empresa, especialmente no que respeita ao sector, à economia, às tendências do Mercado, à tecnologia, às inovações, etc. Para ele, precisará de uma formação multidisciplinar, e isto fará com que a percentagem de Auditores nos departamentos de Auditoria Interna reduza"

Pode ser uma opinião extrema, defendendo que ser bom auditor vem em segundo lugar mas, exemplifica bem a necessidade do conhecimento do negócio e das estratégias para desempenhar adequadamente o trabalho do Auditor.

Em muitos casos os Auditores Internos desempenham um papel fundamental na aplicação de riscos empresariais. Os Auditores Internos podem fazer trabalhos de Auditoria que proporcionem a avaliação objectiva de um processo, quer seja completo ou parcial, da gestão de riscos.

De acordo com as normas do IIA, o alcance da Auditoria Interna deve contemplar a gestão de riscos e os sistemas de controlo, incluindo a avaliação da fiabilidade da informação, a eficiência e eficácia das operações e o cumprimento das leis e regulamentos aplicáveis.

Conforme referido no COSO (2004a), os auditores internos no âmbito das sua funções ajudam a Administração de uma Empresa ou o Comité de Auditoria, analisando, avaliando e informando sobre a adequação e eficácia da gestão de riscos corporativos da organização e na recomendação de melhorias do sistema de gestão de riscos.

[4] Declaración de Posición 2004, El Rol de la Auditoria Interna en la Gestión de Riesgo empresarial; tradução própria

Os Auditores Internos por vezes assumem o papel de consultores, sugerindo melhorias no processo de gestão de riscos corporativos da organização. Nestes casos, os Auditores Internos, podem entre outras actividades promover o desenvolvimento de um conhecimento comum da gestão de riscos corporativos dentro de uma organização, orientar grupos de trabalhos relativos a riscos, bem como, proporcionar ferramentas e técnicas para ajudar a Gestão a analisar os riscos e desenhar actividades de controlo.

Conforme, Sousa (2007) a AI deverá deixar de estar virada essencialmente para garantir a correcta escrituração do passado, sendo muitas vezes vista como um mal necessário, passando a preocupar-se com a consecução dos objectivos e metas da Empresa, através da detecção, análise e gestão dos principais riscos. Deste modo, acrescenta valor, na medida em que contribui para assegurar os resultados esperados são alcançados.

Desta forma o risco passa a assumir uma importância fundamental no processo de Auditoria Interna, devendo ser o centro de toda a actividade, desde o planeamento até à emissão do relatório, passando pela execução e documentação suporte do trabalho realizado (Almeida, 2009).

4.5.Técnicas utilizadas para medir o risco

Não existe um modelo de avaliação do risco que seja standard e como tal aplicado a todas as empresas, pois cada uma tem as suas próprias especificidades, pelo que o Auditor Interno deve ter em consideração as características mais representativas do risco. O importante é conhecer os métodos e a filosofia de medição dos riscos, de modo a poder-se adaptar de acordo com o caso em análise. Contudo, iremos dar um exemplo de como é que se pode medir o risco, partindo do modelo apresentado pela Protiviti, do COSO ERM e da norma AS/NZS 4360;2004.

A medição do risco pode ser feita através de mapeamento do risco, utilizando para o efeito a matriz de risco, conforme exemplo apresentado na figura 5.

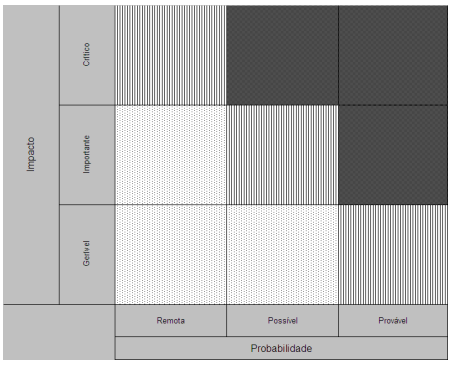


Figura 5**: Matriz de Risco (Fonte:** Protiviti, 2006)

Trata-se de uma matriz de dupla entrada, em que no eixo das abcissas se mede a probabilidade de um determinado risco vir a ocorrer e que foi classificada como remota, possível ou provável. Diz-se que estamos perante uma probabilidade remota, quando não existem perspectivas de que determinado risco ocorra. Uma probabilidade é possível, quando existe um grau de probabilidade que determinado risco venha a acontecer e a probabilidade será considerada provável, quando existe uma forte possibilidade de um risco acontecer.

Suportado numa técnica intuitiva e de simples compreensão e num determinado horizonte temporal (por exemplo 1 ano, 3 anos, etc.), no eixo das ordenadas avalia-se o impacto que o risco pode causar, caso se venha a verificar. O impacto está classificado em gerível, importante e crítico. O impacto é gerível quando o risco ao acontecer, é controlável. O impacto é importante, dado que se trata de um risco que merece alguma atenção pela gestão, porque caso aconteça pode ter consequências desagradáveis na organização. O impacto é crítico, porque é o mais preocupante para a gestão, uma vez que, caso ocorra poderá ter implicações graves e, como tal, merece uma atenção redobrada. Digamos que se trata de uma avaliação em 3 dimensões, horizonte temporal, impacto e a probabilidade de um determinado risco acontecer. A avaliação do impacto e da probabilidade de ocorrência dos riscos de cada processo permite identificar os riscos que apresentam maior criticidade e que exigem uma atenção especial da gestão.

Podem ser utilizadas várias técnicas, nomeadamente recorrendo à linguagem comum, isto é, um instrumento que facilita o diálogo permanente entre os vários intervenientes na gestão de risco de uma empresa, o glossário de riscos, identificação dos riscos aplicáveis, localizar as origens e as fontes de incerteza dos riscos, medir o impacto (gerível, importante ou critico) e o grau de probabilidade (remota, possível e provável), sequenciar os riscos de acordo com a sua importância, considerar potenciais perdas

financeiras, impactos de imagem, reputação da empresa, impacto no cumprimento dos objectivos, entrevistas com pessoas em lugares chave da organização, workshops, aplicação de checklists e análise de histórico.

Uma linguagem comum organiza as informações e dados relacionados com os riscos, as fontes de risco, métricas de risco, análise e comunicação na empresa, bem como, os níveis de processos.

“Utilizando uma linguagem comum, imaginação e um forte conhecimento do processo de negócio, a organização está mais habilitada a alcançar os objectivos do negócio” (Mcnamee, 2000:51).

O COSO ERM (2004a), considera que a avaliação da probabilidade e do impacto do risco pode ser efectuada através de métodos qualitativos e quantitativos e podem ser avaliados individualmente ou por categorias, tendo por base um período temporal. Por regra são utilizados métodos qualitativos, quando os riscos são difíceis de quantificar ou não existe informação suficiente. Os métodos quantitativos são mais precisos e são normalmente utilizados em actividades mais complexas e como complemento ás técnicas qualitativas. A probabilidade e o impacto de um ou mais riscos podem ser representadas graficamente através da utilização de uma matriz de riscos, conforme figura 5.

As directrizes para a implementação da AS/NZS 4360:2004 (Série Risk Management, 2005), refere que as ferramentas de análise permitem que os riscos sejam expressos pela combinação dos seus dois componentes, ou seja, impacto e probabilidade. A relação entre estes dois componentes depende de muitos factores que, por sua vez, reflectem a real natureza do risco e o modo como ele é entendido. Se considerarmos que o nível de risco é proporcional a cada um dos seus dois componentes o risco poderá ser expresso matematicamente como: Risco = Impacto X Probabilidade. De modo a ser possível efectuar uma categorização dos riscos de acordo com o seu grau de criticidade classificamos o impacto e a probabilidade do seguinte modo:

Impacto (Gerível =1, Importante=2; Crítico=3)

Probabilidade (Remota=1; Possível=2; Provável=3).

Refere ainda que podem ser utilizados métodos qualitativos, quantitativos e semi-quantitativos na avaliação dos riscos. A escolha depende em parte do contexto, dos objectivos e dos recursos disponíveis, conforme referido no ponto 3.4.2. Norma Australiana e Neozelandesa (AS/NSZ 4360:2004).

De salientar que, o conhecimento dos processos dos negócios é uma mais-valia na avaliação dos riscos.

A gestão de riscos fecha o ciclo tomando as decisões de gestão que mais se adequam ao risco identificado. Existem várias estratégias que podem ser seguidas na gestão de risco das quais destacamos:

Prevenir Riscos – Esta é uma das melhores estratégias, porque se conseguirmos identificar e prevenir atempadamente quais os eventos negativos que podem acontecer, melhor para a empresa.

Partilhar/Transferir Riscos – É uma forma de gerir riscos. Por exemplo, efectuando contratos com fornecedores ou empresas seguradoras.

Controlar o Risco – Inclui procedimentos de controlo do processo que minimizem as consequências e os efeitos da ocorrência do risco.

5. Aplicação prática: a avaliação do risco num processo de compras

5.1. Metodologia

5.1.1. Objectivos

A apresentação deste trabalho tem como principal objectivo demonstrar, a aplicabilidade de um modelo de gestão de risco nos processos de Auditoria Interna mais especificamente a avaliação dos riscos do negócio que afectam o processo de compras. Neste sentido, efectua-se o levantamento e análise dos riscos dos processos e a avaliação dos respectivos controlos implementados no Departamento de Compras.

Este trabalho permitirá não só introduzir o conceito de gestão de risco na área em estudo como em todas as áreas transversais ao processo de compras, permitindo simultaneamente preparar o trabalho de campo nessas áreas em que a Auditoria Interna virá a realizar em momento posterior.

Desta forma, como resultado final do trabalho será preparada uma matriz de riscos residuais (avaliação dos riscos contemplando a eficácia dos controlos instituídos), devendo ser também apresentadas as principais conclusões da análise aos controlos e respectivas recomendações que na perspectiva da Auditoria Interna contribuem para diminuir o nível de exposição aos riscos analisados, fortalecendo o sistema de controlo interno.

5.1.2. Modelo e fases de aplicação

Este trabalho está sustentado em dois pilares fundamentais, uma das mais conceituadas normas internacionais de gestão de risco, a norma Australiana e Neozelandesa (AS/NZS 4360:2004) e no COSO ERM (COSO, 2004a). Foram utilizadas como ferramenta de apoio a Norma de Gestão de Riscos, (FERMA, 2003), o “Guide to Enterprise Risk Management” (Protiviti, 2006), suportado no COSO nomeadamente, no que diz respeito às matrizes de risco e ao modelo de risco de negócio por eles apresentado, e o “Modelo de Riscos do Negócio”

(PriceWaterHouseCoopers, 2002). O Manual de Riscos de Negócio utilizado neste estudo foi o da PricewaterhouseCoopers, mas com a introdução de algumas adaptações, nomeadamente, a substituição de alguns riscos deste modelo por riscos do modelo apresentado pela Protiviti (2006). De referir que os modelos são bastante semelhantes. Fazem a divisão em três grandes grupos (riscos da envolvente, riscos do processo e riscos financeiros), diferindo apenas em alguns dos riscos específicos apresentados em cada uma das categorias atrás referidas.

Os passos seguidos na aplicação prática por nós apresentada são os referidos na norma Neozelandesa (AS/NZS 4360:2004) e que detalhamos no ponto 3.4.2. Norma Australiana e Neozelandesa (AS/NSZ 4360:2004). De referir que não está no âmbito deste trabalho a aplicação da fase relacionada com Monitorar e Rever. Este ponto poderá ser alvo de desenvolvimento num futuro trabalho sobre este tema.

Iniciamos com a Comunicação e Consulta, uma vez que está associada a todas as fases do processo de gestão de risco e em relação ao processo como um todo, conforme já referido no ponto 3.4.2. Norma Australiana e Neozelandesa (AS/NSZ 4360:2004).

De acordo com a norma, o primeiro passo inicia-se com o **estabelecimento do contexto** interno e externo, o contexto da gestão de risco, desenvolvimento de critérios e definição da estrutura.

Em termos práticos, o estabelecimento do contexto quando aplicado a um processo de negócio de uma organização traduz-se no seguinte:

1. identificação dos processos/sub-processos;
2. identificação e enquadramento nos processos dos objectivos definidos;
3. desenho das principais actividades identificadas em cada um dos processos/sub-processos definidos. Este desenho não necessita de ser realizado de forma detalhada, pretendendo-se apenas a identificação das principais actividades e sistemas de suporte. O desenho poderá ser efectuado através da elaboração de fluxogramas e descritivo das respectivas actividades. De salientar, que devemos evidenciar desde logo as actividades de controlo, uma vez que, esta informação será útil numa fase posterior (avaliação dos controlos).

O passo número dois corresponde à i**dentificação dos riscos**, e basicamente é a resposta a quatro questões, ou seja, o que pode acontecer, quando, onde, como e porquê. Tal como referido abaixo, trata-se de identificar o risco inerente.

Trata-se da identificação dos riscos de negócio que podem existir em cada um dos processos / sub-processos identificados e dentro destes nas principais actividades. Nesta fase do trabalho deve ignorar-se se existem controlos e qual o nível de confiança nos mesmos. Ou seja, pretende-se identificar o risco inerente (o risco que existe para qualquer entidade, na ausência de quaisquer acções que a Gestão venha a tomar, com vista a alterar, quer a probabilidade de ocorrência do mesmo, quer o respectivo impacto). A identificação dos riscos é efectuada com recurso à construção de uma matriz de riscos por processos (Figura 6), classificados de acordo com o impacto e probabilidade de ocorrência dos mesmos;

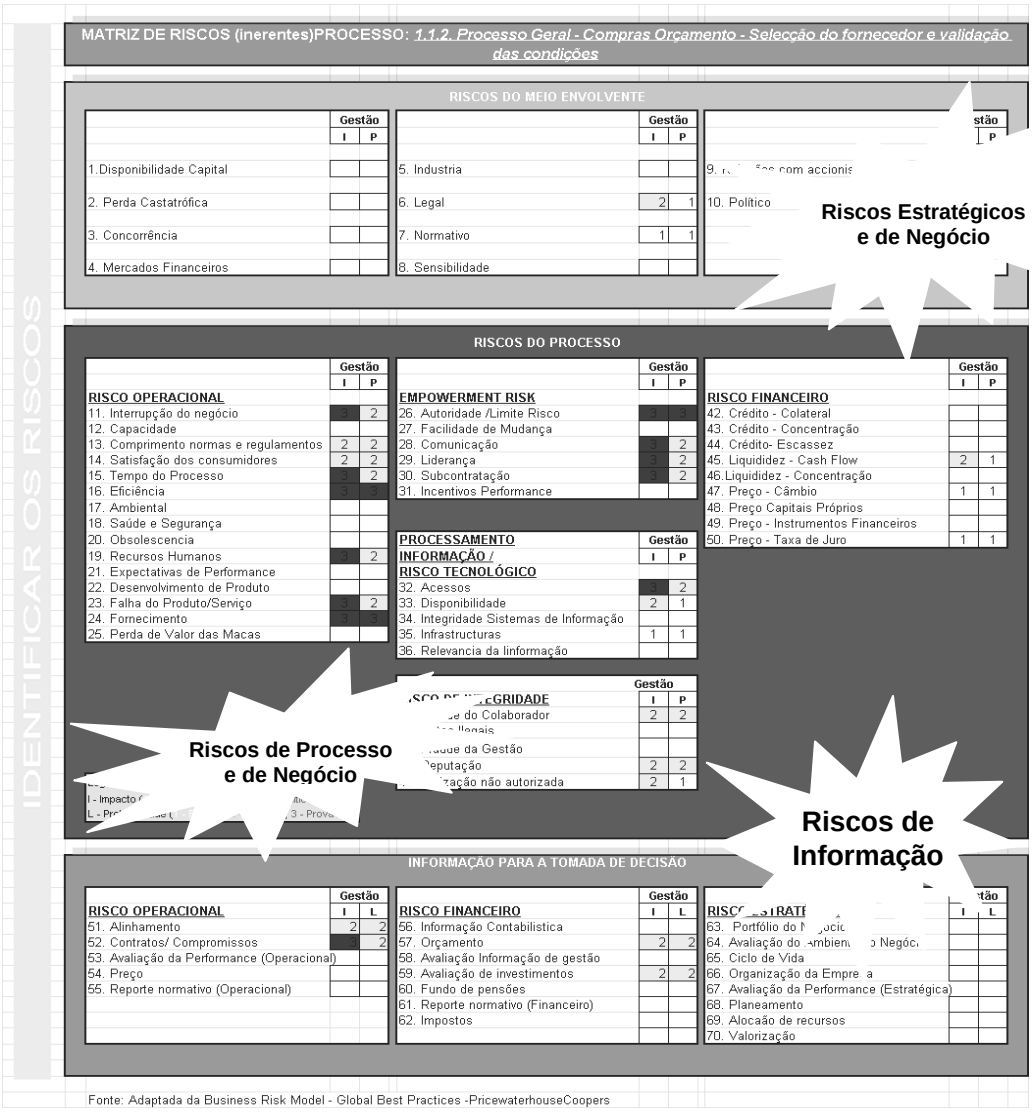


Figura 6: Exemplo de Matriz de Risco (**Fonte:** Adaptado de PricewaterhouseCoopers, 2002)

Na aplicação prática apresentada utilizamos este tipo de matriz para identificar e avaliar os riscos.

O princípio do bom senso aponta-nos para a necessidade de se dispor de uma linguagem dentro das organizações que permita a todos os seus membros utilizá-la sem correrem o risco de serem atribuídos significados distintos pelos diferentes intervenientes no processo. Segundo esta ”linguagem comum” as categorias de riscos estão agrupadas de acordo com as origens da incerteza dos factos que lhes estão na base. As principais fontes de incerteza foram classificadas da seguinte forma:

- **Os riscos da envolvente** que uma empresa enfrenta são originados por realidades do negócio, quer internas, quer externas. São incertezas que afectam a viabilidade do modelo de negócio. Estes riscos ocorrem quando há forças externas que podem por ou põem em causa a continuidade do negócio, ou mudam de forma acentuada os principais pressupostos que conduzem os seus objectivos globais e respectivas estratégias. Estas forças incluem a disponibilidade de capital, as acções dos concorrentes e reguladores, variações ocorridas no mercado, ou outros factos que estejam fora da capacidade da empresa os controlar. Mudanças na envolvente externa podem apresentar ameaças significativas ao negócio.
- **Os riscos de processo** são incertezas que afectam a execução do modelo de negócio. Estes riscos acontecem quando os processos utilizados no negócio não atingem aquilo para que foram desenhados. Alguns exemplos de características de processos deficientemente desenhados, ou “riscos de processo”, podem ser:
    - O processo não está alinhado de forma eficaz com as estratégias globais, é ineficaz no tocante á satisfação das necessidades dos clientes, não funciona de uma forma operacionalmente eficaz e não resulta na criação de riqueza.
    - O processo falha no que à protecção de perdas inaceitáveis diz respeito, isto é, falha na tomada de decisão ou uso indevido de activos financeiros, intelectuais e físicos.

  Incluído nos riscos de processo está o risco de processamento da informação/risco tecnológico, o qual ocorre quando as tecnologias de informação utilizadas no processo não estão a funcionar, tal como planeado,

ou estão a comprometer a disponibilidade, integridade e segurança da informação e de outros activos.

- **Risco relativo à informação** são incertezas sobre a relevância e fiabilidade da informação. Estes riscos ocorrem quando a informação utilizada para apoiar a tomada de decisão é incompleta, desactualizada, pouco precisa, atrasada ou irrelevante. Neste campo a maior parte das empresas reconhece que os sistemas de apoio à decisão estão longe daquilo que seria o óptimo. Este risco é directamente afectado pela eficácia e segurança dos sistemas de processamento da informação e de processos informais de recolha de "informação confidencial" no que à captura de informação relevante diz respeito, convertendo as notícias em informação e fornecendo essa informação aos gestores apropriados, na forma de relatórios tempestivos e de comunicações verbais.

São estas as três categorias de riscos do negócio que, por sua vez, proporcionam uma ampla base a partir da qual riscos mais específicos podem ser identificados e detalhados, conforme se pode ver no manual de riscos do negócio em anexo (Anexo 1).

Tal como nos riscos da envolvente ao negócio, a mudança constante tem impacto em todas as categorias do risco do processo. A reengenharia de processos, a subcontratação, alterações nos volumes de vendas, mudanças efectuadas na estrutura organizacional, alterações ao nível de pessoal, implementação de novos sistemas de informação, fusões, aquisições e reorganizações empresariais são exemplos de mudanças indicativas de potenciais riscos de processo.

Os riscos de processo são muitas vezes não distinguíveis de informações para a tomada de decisão, uma vez que a informação é necessária para se tomarem decisões esclarecidas acerca de um processo. Um fluxo contínuo de informação deveria dotar os decisores com as perspectivas que necessitam acerca da envolvente e da performance dos processos utilizados pela empresa de tal modo que possam gerir os riscos da organização de forma eficiente.

A matriz de risco de processo vai permitir fazer a identificação e avaliação dos riscos dos processos. Depois de identificados os riscos passa-se à fase de análise. Nesta fase é feito o mapeamento dos riscos absolutos, isto é, representar numa Matriz os Riscos Inerentes (Figura 7), posicionando-os de acordo com a sua gravidade, isto é,

de acordo com a classificação obtida em resultado da multiplicação do Impacto pela Probabilidade e obtemos a Matriz de Risco Inerente (Figura 7 e 8).

Entende-se por **Risco inerente/absoluto**, o risco que existe para qualquer entidade, na ausência de quaisquer acções que a Gestão venha a tomar, com vista a alterar, quer a probabilidade de ocorrência do mesmo, quer o respectivo impacto.

Processos / Riscos		6. Legal	7. Normativo	11. Interrupção do negócio	13. Cumprimento normas e regulamentos	14. Satisfação do Consumidor	15. Tempo do Processo	16. Eficiência
1.1. Compras Orçamento	1.1.2. Selecção do fornecedor e validação das condições	2	1	6	4	4	6	9
	1.1.4. Criação do Acordo de Fornecimento	1	1	6	1		6	4
	Nº Ocorrências	2	2	2	2	1	2	2
	Nº Ocorrências [Risco Abs. >3]	0	0	2	1	1	2	2

Figura 7: Excerto Mapa dos Riscos Inerentes (**Fonte:** Produção própria)

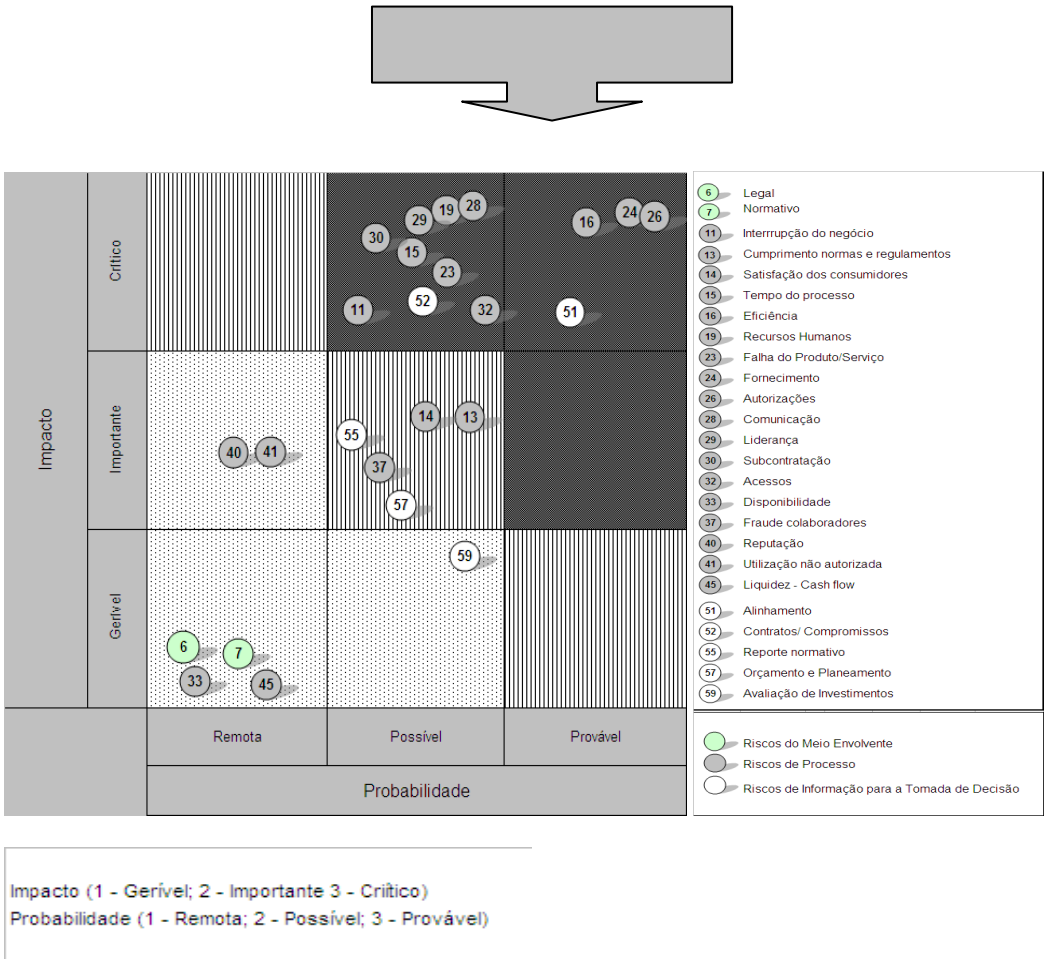


Figura 8: Matriz Risco Inerente (**Fonte:** Adaptado de Protiviti, 2006)

Para a realização deste trabalho conjunto de análise e avaliação dos riscos, socorremo-nos de:

- Uma linguagem comum (riscos agrupados de acordo com a origem das incertezas que lhes estão na base) e,
- Uma metodologia para tipificação dos riscos e sua caracterização (glossário, matriz e mapeamento dos riscos).

Os riscos foram classificados de acordo com o nível de:

- Impacto – ou seja, qual a magnitude que determinado risco teria, se viesse a ocorrer (o impacto pode ser em muitas áreas, incluindo a financeira, a da imagem/reputação, ao nível dos recursos humanos, sobre a valorização das existências, etc.), e
- Probabilidade – dadas as inerentes incertezas do negócio, qual será a probabilidade que determinado risco tem de poder ocorrer.

Em termos práticos esta análise pode ser feita do seguinte modo:

- Construção da lista de actividades críticas por processo a avaliar e testar;
- Definir um programa detalhado de identificação, avaliação e execução de testes aos controlos nas actividades com risco e probabilidade de ocorrência mais elevados;

Concluída a fase da análise dos riscos e avaliação dos controlos, ou seja, depois de identificados e avaliados os controlos existentes, passamos à fase de identificação dos riscos residuais.

Os riscos são reavaliados considerando os resultados dos testes efectuados, tendo em conta a capacidade que os controlos implementados têm para mitigar os riscos identificados, associados aos processos, determinando-se assim o risco residual.

A avaliação dos riscos de processo com base nos resultados dos testes efectuados e construção de uma matriz final dos riscos de processo de acordo com os resultados da avaliação aos controlos, ou seja, a matriz do risco residual (Figura 9), isto é, aquele que permanece depois de implementados os controlos e medidas de redução do risco. O objectivo óptimo será que o risco residual tenda para zero.

Segundo Silva (2006) o papel da Auditoria Interna vai centrar-se na diferença entre o risco inerente e o residual:

"É na análise da diferença entre o risco inerente e o residual que a Auditoria Interna deverá ter particular interesse pois através dela se constatará se o sistema de controlo interno funciona e se a gestão é eficaz fazendo com que o sistema de acumulação da empresa continue a funcionar de uma forma sustentada", **Silva (2006:12).**

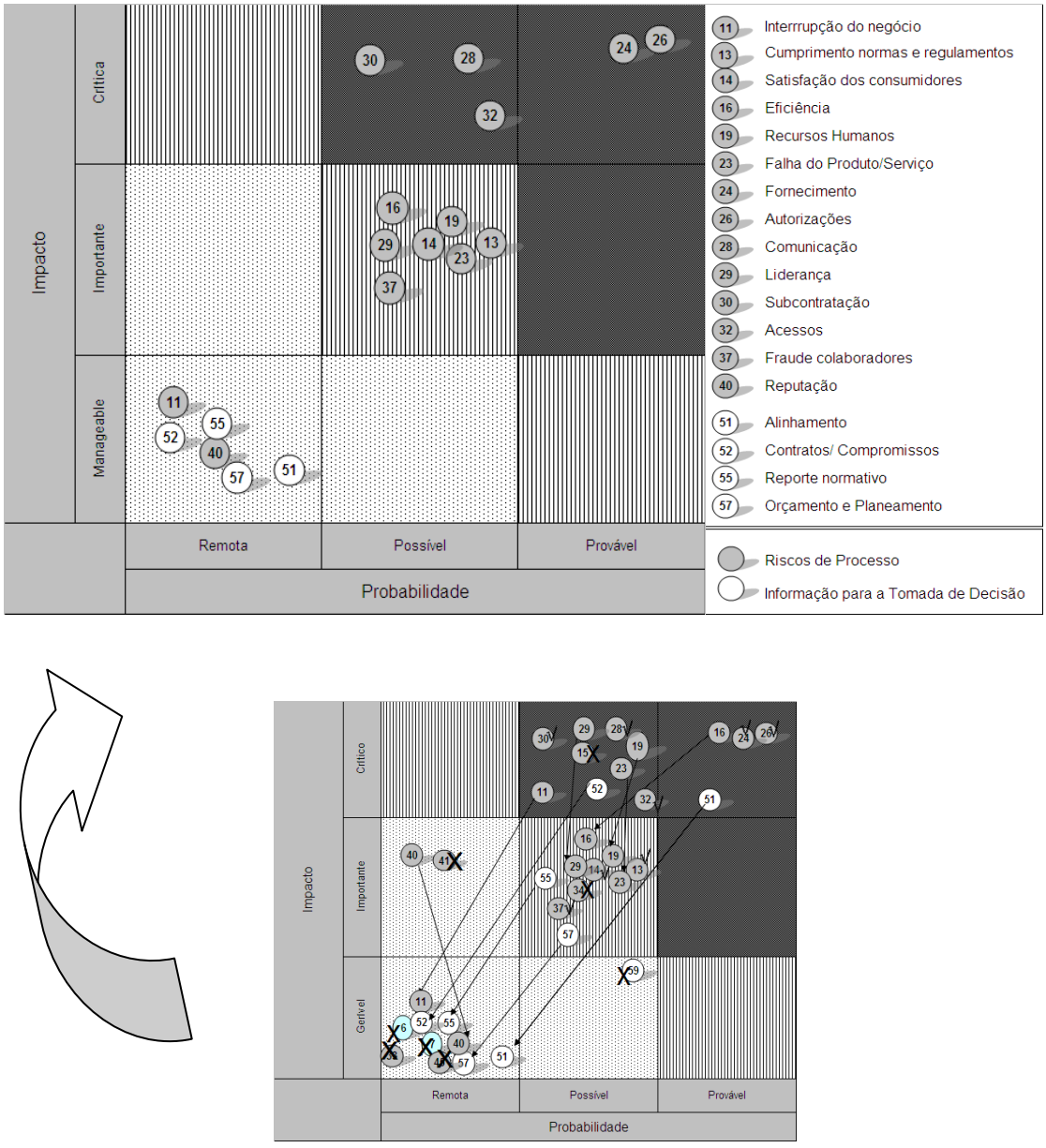


Figura 9: Passagem da Matriz de Risco Inerente para a Matriz de Risco Residual **(Fonte:** Adaptado de Protiviti, 2006)

Depois de identificados os riscos residuais deve ser promovida uma discussão dos riscos, ocorrências e controlos com o grupo de trabalho, em workshops e apresentação das recomendações e propostas de melhoria, de modo a que todas as

pessoas envolvidas no trabalho possam pronunciar-se sobre as conclusões a que chegamos e as respectivas recomendações de melhoria. O objectivo destas reuniões de trabalho é que Auditoria e área Auditada estejam de acordo quanto à avaliação dos riscos e recomendações propostas.

Face à avaliação realizada sobre os controlos, a lista dos principais riscos inicialmente calculada, tendo como referência o risco absoluto, sofreu naturalmente algumas mudanças tendo mesmo ocorrido a saída de alguns riscos dessa lista e entrado outros que, inicialmente, não se consideravam tão relevantes.

Determinados os riscos residuais do processo e após consenso com a área auditada, vão ser definidas medidas para mitigar os riscos e definidos planos de acção.

Nesta fase é que se decide como é que vão ser tratados os riscos, ou seja, se vão ser transferidos ou partilhados, por exemplo através da contratação de seguros, se vão ser controlados e aceites ou, ainda, se a opção passa por diversificar ou evitar.

Nesta fase deve ser efectuado um workshop, onde se faz uma apresentação à área auditada. Este workshop tem como objectivo discutir as conclusões obtidas de acordo com a percepção e avaliação dos riscos feita pela Auditoria Interna, de modo a que haja consenso entre as duas áreas.

Devem ser definidas medidas que mitiguem o risco, estabelecido um calendário e definidos os intervenientes para a sua implementação.

O processo de avaliação dos riscos engloba três fases: i) Identificação dos Riscos, ii) Análise dos Riscos e iii) Avaliação dos Riscos.

Na fase do Tratamento dos Riscos é definido o plano de resolução e implementação pela gestão em parceria com a Auditoria Interna, que vai agir como facilitador e avaliador da qualidade dos controlos a implementar face aos objectivos definidos;

As fases de Monitorar e Rever, serão aplicadas em momento posterior, uma vez que, visam verificar se as medidas propostas para a mitigação dos riscos identificados como passíveis de serem tratados, foram ou não implementadas. Caso tenham sido implementadas é necessário confirmar que as mesmas são eficazes na mitigação desses mesmos riscos. O resultado deste trabalho é posteriormente comunicado ao Responsável da área auditada e à Gestão.

Caso as medidas tenham sido implementadas mas se revelem pouco ou nada eficazes, deve proceder-se à identificação de novas medidas de modo a que se consiga o objectivo, ou seja, a mitigação dos riscos.

Esta fase, não é estática, deve-se fazer uma monitorização e um acompanhamento periódico, de modo a verificar se os controlos foram bem implementados e são eficazes e, por outro lado, verificar se surgiram novos eventos que necessitem de ser analisados e acompanhados, razão pela qual é importante a análise crítica e a repetição regular do ciclo de gestão de riscos.

Deve ser feita uma análise crítica contínua de modo a assegurar que as medidas correctivas propostas foram correctamente implementadas e são eficazes na mitigação dos riscos identificados e para os quais foi aprovada a implementação das recomendações sugeridas pela Auditoria Interna.

Os resultados obtidos na monitorização são posteriormente comunicados à área auditada e à gestão.

5.1.3. Universo utilizado para aplicação do modelo

O caso prático apresentado, aplica-se a um grupo empresarial (industrial e comercial), de grande dimensão, que ocupa lugar de destaque no sector em que opera, quer no mercado nacional, quer no mercado internacional.

Para efeito deste estudo vamos limitar o âmbito do trabalho de Auditoria, focalizado na gestão de risco, ao processo de compras. Contudo, tendo em consideração a dimensão deste processo, restringimos o nosso trabalho ao sub-processo compras orçamento (materiais de embalagem). Optámos pelos materiais de embalagem, pelo facto, dos mesmos representarem cerca de 50% do total das compras realizadas neste departamento.

5.1.4. Pressupostos

Tendo em consideração a complexidade do processo e o objectivo deste trabalho, vamos limitar o âmbito, utilizando os seguintes pressupostos:

- Trabalho realizado no âmbito do plano anual de auditoria aprovado pelo Comité de Auditoria. O plano de auditoria é realizado, tendo em consideração os riscos do negócio e os objectivos estratégicos da empresa.
- Não obstante o processo de compras estar interligado com diferentes áreas da empresa a nossa aplicação incide apenas nas actividades desenvolvidas na

área de Compras, pelo que, fica fora do âmbito deste trabalho o levantamento e análise dos processos das áreas transversais ao processo em análise;

- As técnicas de Auditoria utilizadas na realização deste tipo de trabalho de Auditoria de Processos, são regra geral, as entrevistas e questionários efectuados aos responsáveis e colaboradores da área auditada, permitindo deste modo efectuar o levantamento e desenho dos processos em análise, caso a área não disponha desta informação, bem como, a recolha e análise de informação gerada nos processos avaliados e a realização de testes de conformidade;
- Foram desenhados programas de testes de conformidade essencialmente para avaliação dos controlos transaccionais (considerando a eficiência/eficácia das operações, cumprimento de leis e regulamentos e reporte de informação financeira/performance).

Todo o trabalho é desenvolvido no pressuposto de que a organização dispõe de um manual de procedimentos de controlo interno.

5.2. Aplicação da avaliação de risco num processo de compras

Partindo dos passos descritos no ponto anterior vamos aplicá-los ao processo de compras. Iniciamos com o estabelecimento do contexto que engloba vários aspectos: compreender o contexto estratégico, compreender os processos de negócio e estabelecer uma linguagem comum. De seguida, passamos ao processo de avaliação dos riscos com a apresentação das respectivas matrizes. Por último, apresentamos a fase do tratamento dos riscos.

5.2.1. Estabelecimento do Contexto

Como vimos no ponto 5.1.2 Modelo e fases de aplicação, o estabelecimento do contexto corresponde ao primeiro passo do processo de gestão de risco. Desta forma, é a fase onde se faz o enquadramento do trabalho de análise e avaliação dos riscos e controlos, caracterizando-se pelo estabelecimento dos parâmetros básicos que definem o âmbito da nossa análise e pela definição dos critérios a considerar na avaliação do risco dentro desse contexto.

Esta definição do contexto inclui a identificação das áreas de negócio que se consideram ter maior intervenção nos processos de compras, a identificação dos objectivos de negócio relacionados com esta área (seguindo o referido no ponto 2.4.) e a definição dos parâmetros considerados na qualificação dos riscos quanto ao impacto e probabilidade de ocorrência (avaliação do risco). Logo, engloba três elementos básicos: compreender o contexto estratégico, compreender os processos de negócio e estabelecer uma linguagem ou modelo comum (figura 10).

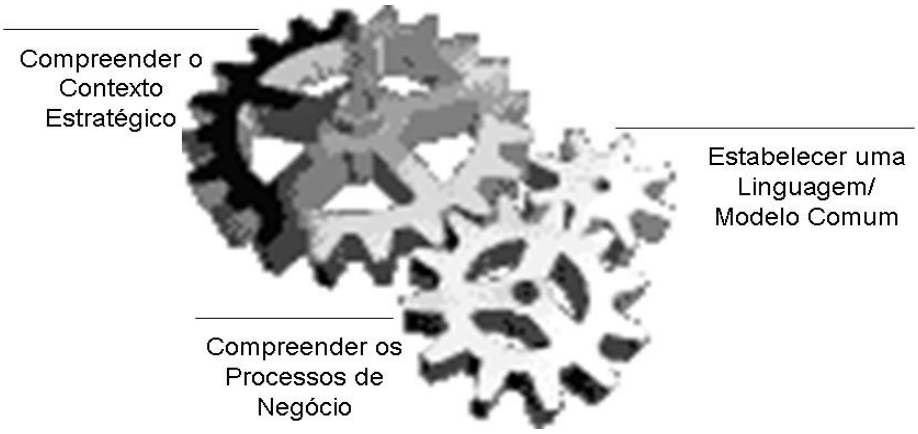


Figura 10: Estabelecimento do Contexto (**Fonte:** Produção Própria)

Este passo constitui a base de suporte das conclusões apresentadas neste trabalho e que vão, naturalmente, influenciar todo o processo de gestão dos riscos que venha a ser conduzido em função dos resultados apresentados.

5.2.1.1. Compreender o contexto estratégico

Sendo o nosso estudo relativo à aplicação da gestão de risco a um processo de compra, a compreensão do contexto estratégico ao nível mais específico, prende-se com a envolvente do Departamento de compras. Assim, para que se possa realizar uma correcta avaliação dos riscos de negócio que afectam os processos desenvolvidos no âmbito de actuação da Departamento de Compras, é necessário compreender os objectivos, responsabilidades e modelo organizacional desta área.

5.2.1.1.1. Caracterização do Departamento de Compras

O Departamento de Compras deve garantir os processos de compra de todos os materiais, bens e serviços, nas melhores condições de preço, serviço e qualidade, assegurando a satisfação das necessidades apresentadas pelas diferentes áreas da

organização, tendo sempre como principal objectivo diminuir custos e maximizar o valor da empresa.

As Principais responsabilidades do Departamento de Compras são:

- Comprar todos os materiais, bens e serviços externos, de acordo com as necessidades das diferentes áreas da organização, com excepção de compras específicas que requerem a intervenção directa da própria área requisitante enquadrando-se no âmbito de actividade de Compras Delegadas.
- Efectuar uma procura regular, nos mercados interno e externo, de fornecedores adequados às necessidades das diferentes áreas da organização;
- Manter actualizado o “Sistema de Avaliação de Fornecedores” e utilizá-lo como ferramenta de apoio à decisão, identificação e selecção dos principais fornecedores;
- Garantir a gestão eficaz das bases de dados do sistema informático, em concreto do “Ficheiro Mestre de Materiais” e do “Ficheiro Mestre de Fornecedores”

As compras podem ser classificadas em grandes grupos de acordo com diferentes critérios. Cada um dos grupos pode representar distintos pesos no valor total dos gastos incorridos e na sua importância para o negócio. Uma classificação possível é de acordo com o destino dos bens e serviços comprados resultando, por exemplo, os seguintes grupos de compras: Industrial, Matérias-primas, Químicos, Material de Embalagem e Serviços Diversos.

A classificação e o peso de cada um dos grupos depende muito de empresa para empresa. Para a realização deste trabalho, como vimos, considerámos uma Empresa Industrial e Comercial em que o grupo com maior peso no total de compras desta empresa é o de materiais de embalagem (representam cerca de 50% do total das compras desta empresa), razão pela qual foi seleccionado para o trabalho.

A actividade de compras deve ser exercida de acordo com um conjunto de princípios gerais, que devem estar descritos no Manual de Procedimentos de Controlo Interno, nomeadamente, no que diz respeito à eficiência organizativa, minimização de custos, eliminação de conflitos de interesses, respeito pelas normas éticas, garantia do cumprimento dos normativos e atitude positiva e de responsabilidade.

5.2.1.1.2. Políticas e Procedimentos internos aplicáveis

É importante a Auditoria Interna ter conhecimento dos manuais existentes na Organização, nomeadamente, o Manual de Qualidade e o Manual de Procedimentos de Controlo Interno. Estes manuais são as duas principais referências na aplicação das normas e procedimentos neste processo, caso a empresa disponha deles.

O Manual de Qualidade está inserido no Sistema de Gestão da Qualidade, Ambiente e Segurança cabendo a responsabilidade pela sua manutenção à área de Qualidade, que promove também a realização de auditorias neste âmbito. Estamos a falar de uma empresas certificada.

O Manual de Procedimentos de Controlo Interno define as Políticas e Procedimentos de Controlo Interno adoptados pela empresa. É conveniente que os manuais se encontrem actualizados.

5.2.1.2. Compreender os processos de negócio

Nesta fase importa conhecer os processos principais e os de suporte das compras e entender de que forma estes processos se enquadram na estrutura organizativa.

5.2.1.2.1. Processos principais e de suporte às Compras

Lorenzo (2001), define processo da seguinte forma:

> "é um conjunto estruturado de actividades organizadas desenhadas para alcançar um ou vários objectivos e conta sempre com pelo menos um intput e um output. Os processos podem dividir-se em sub-processos, sendo que estes são formados por actividades que por sua vez se desdobram em tarefas"[5] (Lorenzo, 2001:79).

Assim, quando se pretende analisar um processo dever-se-á começar pela decomposição do mesmo nos seus três principais níveis hierárquicos (processo, sub-processo e actividade). Neste trabalho, dada a complexidade e diversidade de actividades envolvidas, apenas nos focalizaremos ao nível do processo e sub-processo.

[5] Tradução própria

Para compreender os processos de negócio ligados às compras procedemos à identificação e caracterização dos processos principais que suportam o Departamento de Compras e que se encontram esquematizados na figura 11.

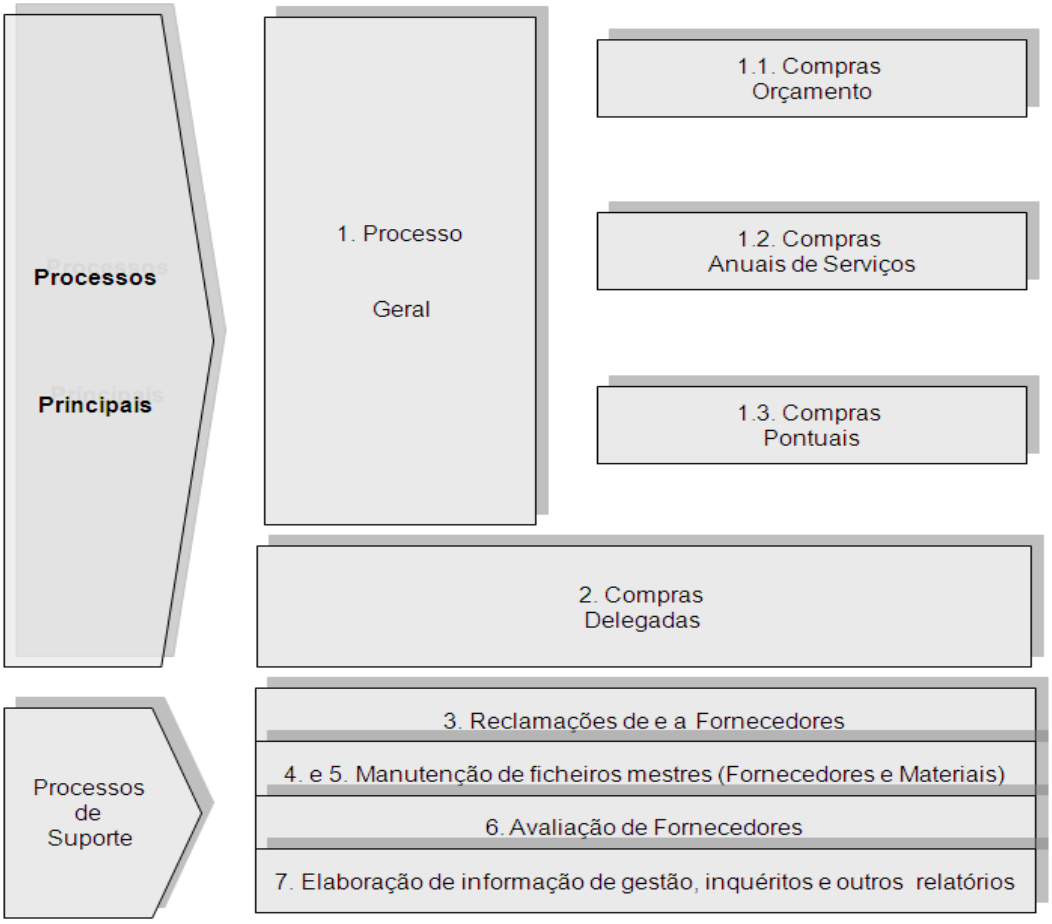


Figura 11: Processos principais e processo de suporte – Compras (**Fonte:** Produção Própria)

O desenho de um adequado sistema de controlo interno requer conhecer inicialmente quais são os processos principais e sub-processos do negócio, (Martín e Morales, 2001). Assim, no âmbito de intervenção em que a análise do risco deverá ocorrer é necessário uma desagregação por processos principais , processos de suporte e sub-processos, que é visível na figura 11. Daqui resultam dois processos principais, processo geral e compras delegadas; e cinco processos de suporte: reclamações de e a fornecedores, manutenção de ficheiros mestres (Fornecedores e Materiais), avaliação de fornecedores e elaboração de informação de gestão, inquéritos e outros relatórios. De seguida passaremos a explicar os diferentes processos.

5.2.1.2.1.1. Processos principais

O Macro processo do Departamento de Compras está dividido em processos principais e processos de suporte e controlo. Foram identificados dois processos de negócio, o Processo Geral de Compras, ou seja, o processo normal de compras que envolve a participação do Departamento de Compras com níveis de intervenção diferenciados, tendo em consideração o tipo de material e as suas especificidades que podem subdividir-se em Compras Orçamento, Compras Anuais de Serviços e Compras Pontuais.

Nas Compras Orçamento estão incluídos os Acordos de Fornecimento Anuais (ou até por períodos superiores) efectuados com base nos orçamentos anuais de consumos de materiais em quantidades e valor. Estes orçamentos são função dos programas de vendas elaborados pela área comercial, normalmente em Setembro, para o ano seguinte. Os orçamentos são enviados pelas diferentes áreas de negócio para o Departamento de Compras, conforme se pode ver na figura 12. São exemplos de compras orçamento, as compras de materiais de embalagem e de matérias-primas.

A análise dos processos recorrendo à utilização de fluxogramas facilita a detecção de pontos de risco.

O processo inicia-se com a prospecção de novos fornecedores no mercado. Com base nesta prospecção o gestor de compras actualiza a lista de fornecedores e consequentemente o ficheiro mestre de fornecedores.

De salientar que, os fornecedores considerados relevantes para a qualidade têm de ser aprovados pela Direcção de Qualidade, ou seja, todos aqueles cujo material tenha contacto directo com o produto, como é o caso dos materiais de embalagem. Assim, só depois de aprovados serão incluídos no cadastro de fornecedores, encontrando-se disponíveis para efectuar pedidos de cotação.

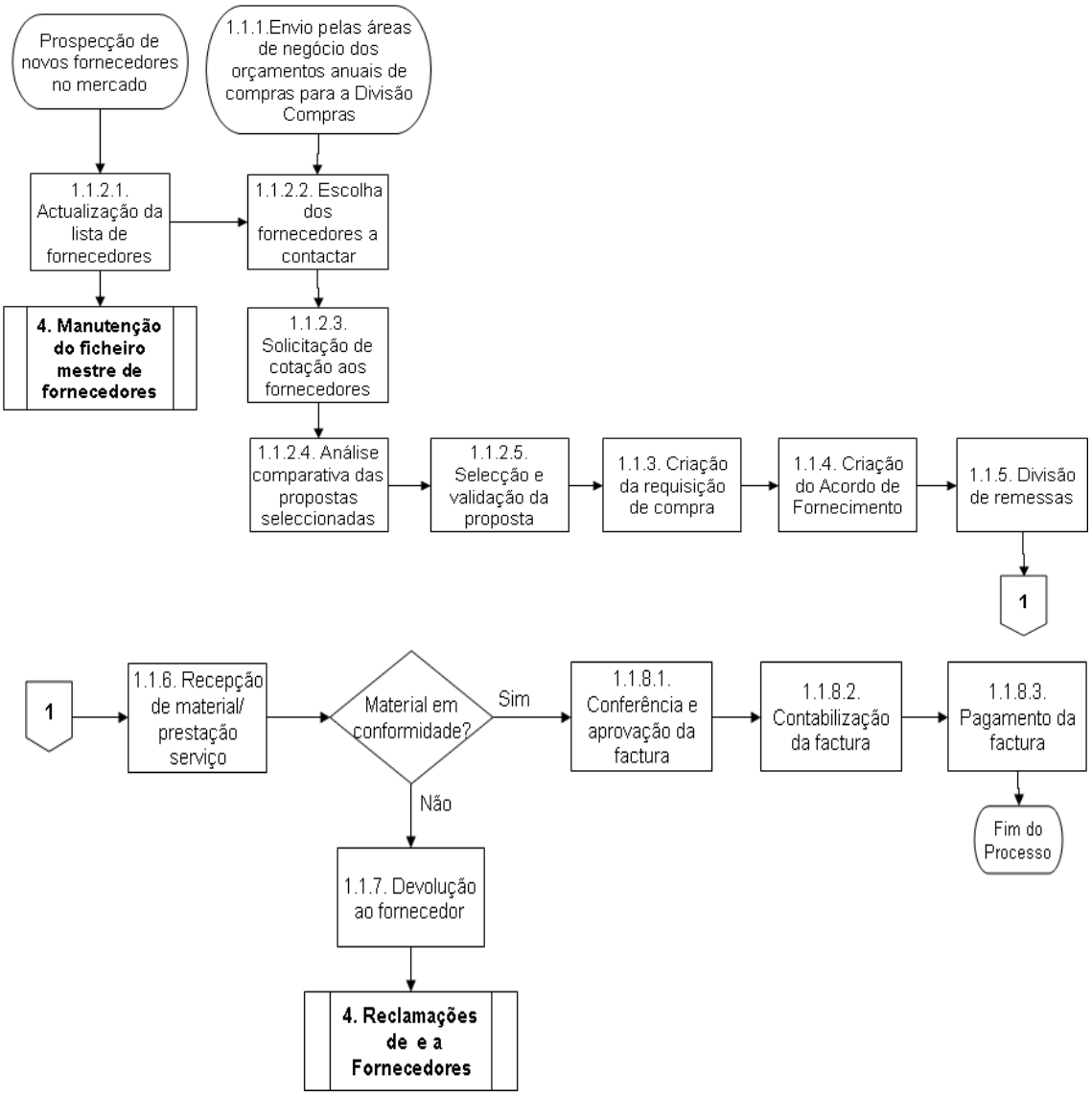


Figura 12: Fluxograma do Processo Compras Orçamento (**Fonte:** Produção própria)

O Departamento de Compras, com base na informação dos orçamentos de compras enviados pelas respectivas áreas operacionais, selecciona os fornecedores a contactar e solicita cotações. De acordo com os procedimentos internos devem ser solicitadas propostas a pelo menos três fornecedores. Recepcionadas as propostas, o gestor de compras faz uma análise comparativa permitindo-lhe avaliar e apresentar a proposta mais favorável para validação superior. Seleccionado o fornecedor, o gestor de compras informa a área requisitante para que seja efectuada a requisição de compra. Com base na requisição de compra o gestor de compras cria o acordo de fornecimento.

Posteriormente, a área operacional faz a divisão de remessa, isto é, encomenda de acordo com as necessidades, uma vez que o acordo vigora para o período de um ano e é feito pela totalidade das quantidades orçamentadas. A encomenda é satisfeita pelo fornecedor e a área requisitante procede à recepção dos materiais / serviços.

O Controlo de Qualidade verifica se os materiais estão em conformidade, caso se trate de materiais relevantes para a qualidade, caso contrário a validação é efectuada pela área requisitante. Caso não estejam conforme, os materiais são devolvidos e é feita uma reclamação ao fornecedor. Se os materiais corresponderem ao pretendido e estiverem em conformidade é efectuada a conferência da factura e solicitada a aprovação superior, passando-se à sua contabilização para posterior pagamento na data de vencimento, concluindo assim o processo.

As Compras Anuais de Serviços dizem respeito à contratação de serviços anuais, avenças mensais, nas quais se conhecem os valores a pagar mensalmente até ao fim do ano. Apresenta-se na figura 13 o fluxograma do processo de compras de serviços nas quais se incluem, por exemplo, os serviços de limpeza, de vigilância e de manutenção.

Conforme se pode ver no fluxograma apresentado abaixo, em termos de processo é idêntico ao das compras orçamento, apenas difere no modo como é formalizada a compra, ou seja, nas compras orçamento utiliza-se a figura de acordo de fornecimento (contrato), enquanto que nas compras anuais de serviços é criada uma encomenda anual. Esta questão prende-se essencialmente com o tipo de compra e de negociação que é efectuada.

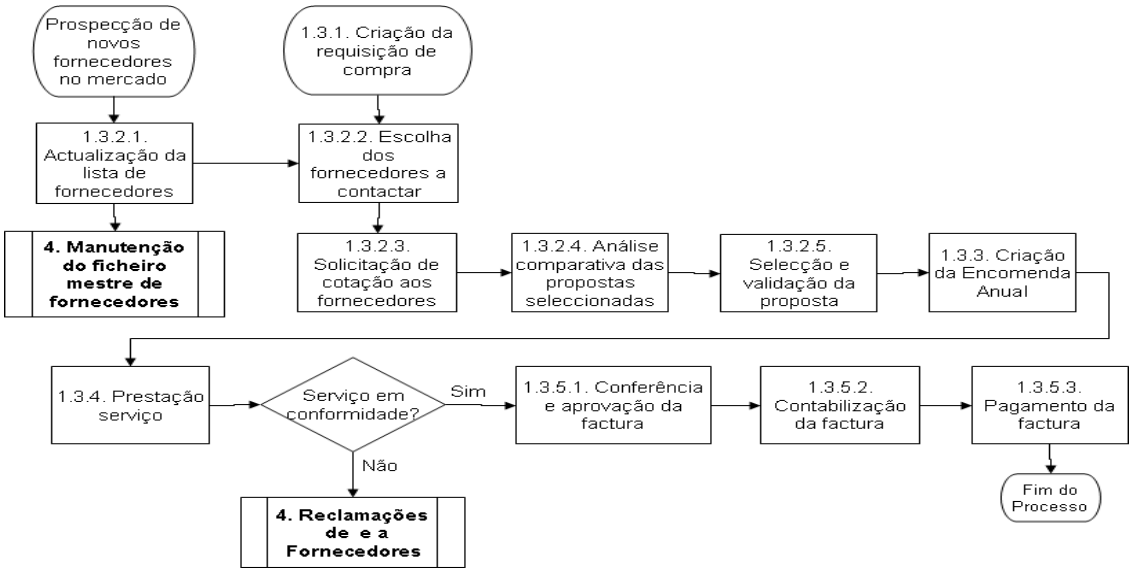


Figura 13: Fluxograma do Processo de Compras de Serviços (**Fonte:** Produção própria)

As Compras Pontuais, por exclusão de partes, estão relacionadas com a compra de materiais/serviço que não se enquadram nos restantes processos devido à reduzida significância, à urgência da compra, ao seu carácter esporádico ou ainda às particularidades do material/serviço requisitado. Neste caso, é criada uma encomenda normal, sendo que o restante processo é idêntico aos referidos anteriormente. A figura 14 apresenta o fluxograma correspondente a este tipo de compras.

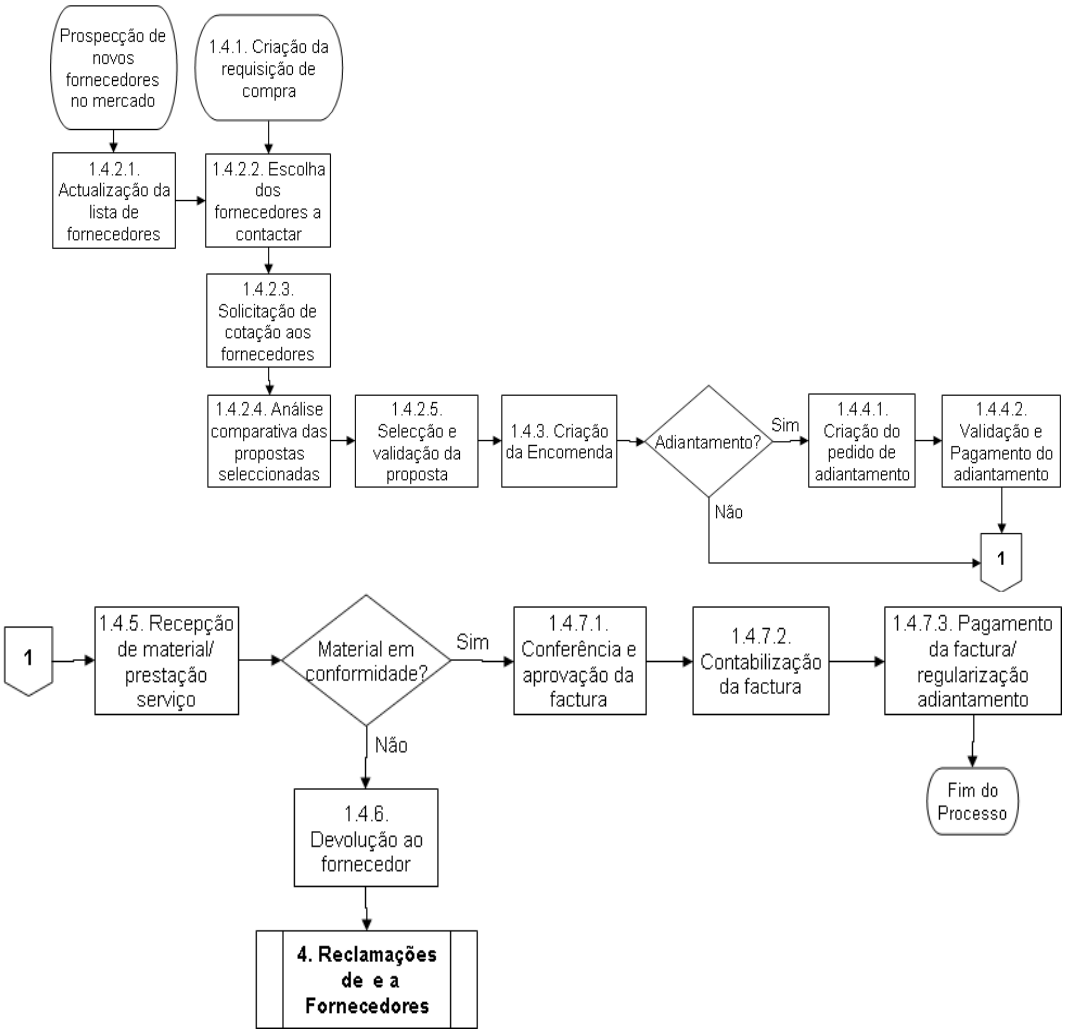


Figura 14: Fluxograma do Processo de Compras Pontuais (**Fonte:** Produção própria)

O segundo processo de negócio foi designado por Compras Delegadas e refere-se às compras efectuadas directamente pelas Áreas Operacionais sem qualquer intervenção da Área de Compras. Regra geral, trata-se de compras de materiais/serviços muito específicos, sujeitas a especificações próprias, que requerem intervenção directa da própria área requisitante, uma vez que, as pessoas que fazem parte do Departamento

de Compras não dispõem dos conhecimentos necessários para fazer estas aquisições. A figura 15 apresenta o fluxograma relativo a este tipo de compras. São exemplo de compras delegadas os transportes de mercadorias, materiais destinados a acções de marketing e comunicação.

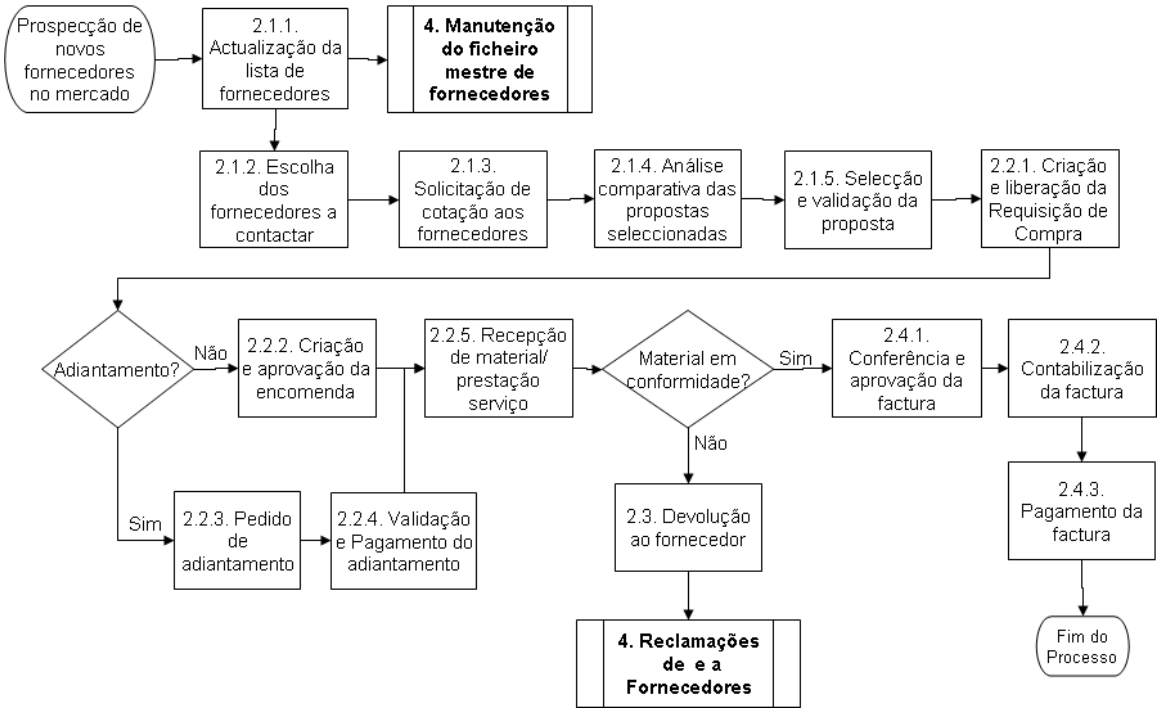


Figura 15: Fluxograma do processo de Compras Delegadas (**Fonte:** Produção Própria)

5.2.1.2.1.2. Processos de suporte às Compras

Foram identificados cinco processos de suporte, reclamações a e de fornecedores, manutenção de ficheiros mestres de fornecedores e de materiais, avaliação de fornecedores, elaboração de informação de gestão, inquéritos e outros relatórios.

As reclamações a e de fornecedores, compreende as actividades desenvolvidas pela área de Compras no âmbito de reclamações que possam surgir na sequência do não cumprimento do acordo por qualquer uma das partes.

No que diz respeito à manutenção de ficheiros mestres de fornecedores consideram-se todas as actividades relacionadas com a manutenção da informação dos dados mestre de fornecedores no sistema de informação (criação de novos fornecedores, alteração de dados dos já existentes, actualização da base de dados, etc.).

A manutenção de ficheiros mestres de materiais diz respeito a todas as actividades relacionadas com a manutenção da informação dos dados mestre de materiais no sistema de informação, nomeadamente a criação de novos materiais, alteração/eliminação de materiais já existentes, etc.

A avaliação de fornecedores, trata-se do processo de avaliação e acompanhamento dos fornecedores ao longo do ano. A avaliação dos fornecedores é efectuada tendo em consideração vários parâmetros, nomeadamente, se os materiais fornecidos estão de acordo com as especificações indicadas, se passou nos testes efectuados pelo controlo de qualidade, se a recepção dos materiais foi efectuada dentro do prazo acordado, etc.

Estas avaliações tem como principal objectivo, identificar os fornecedores que ao longo do ano não cumpriram com todos as suas obrigações, avaliando os impactos que tiveram na empresa, de modo, a que sejam definidas e implementadas medidas correctivas, que podem passar pela substituição do fornecedor. Por regra, apenas são informados da avaliação os fornecedores que não cumpriram com as suas obrigações, de modo, a alerta-los para o sucedido e tentarem junto dos mesmos identificar quais as razões de tal incumprimento, de modo a que sejam evitadas no futuro. Por outro lado, e tendo em consideração a gravidade das situações, poderá a empresa optar por recorrer a novas pesquisas no mercado e seleccionar fornecedores alternativos.

O processo de elaboração de informação de gestão, inquéritos e outros relatórios compreende toda a informação de gestão desenvolvida pelo próprio Departamento de Compras, bem como, resposta a inquéritos de entidades externas. Trata-se de informação específica, nomeadamente, análise de indicadores de rentabilidade e performance da própria área.

5.2.1.2.2. Enquadramento dos processos na Estrutura Organizativa

Os processos relacionados com as Compras são transversais a toda a organização, tocando por isso mesmo as mais diversas áreas do negócio. É, portanto, necessário identificar de que forma se enquadra na estrutura da Organização e qual o grau de intervenção de cada área para que possa ser desenvolvida uma análise adequada dos riscos e uma correcta identificação e avaliação dos controlos implementados.

A matriz a seguir apresentada (figura 16) pretende demonstrar de que forma os processos identificados envolvem a participação das várias área da organização.

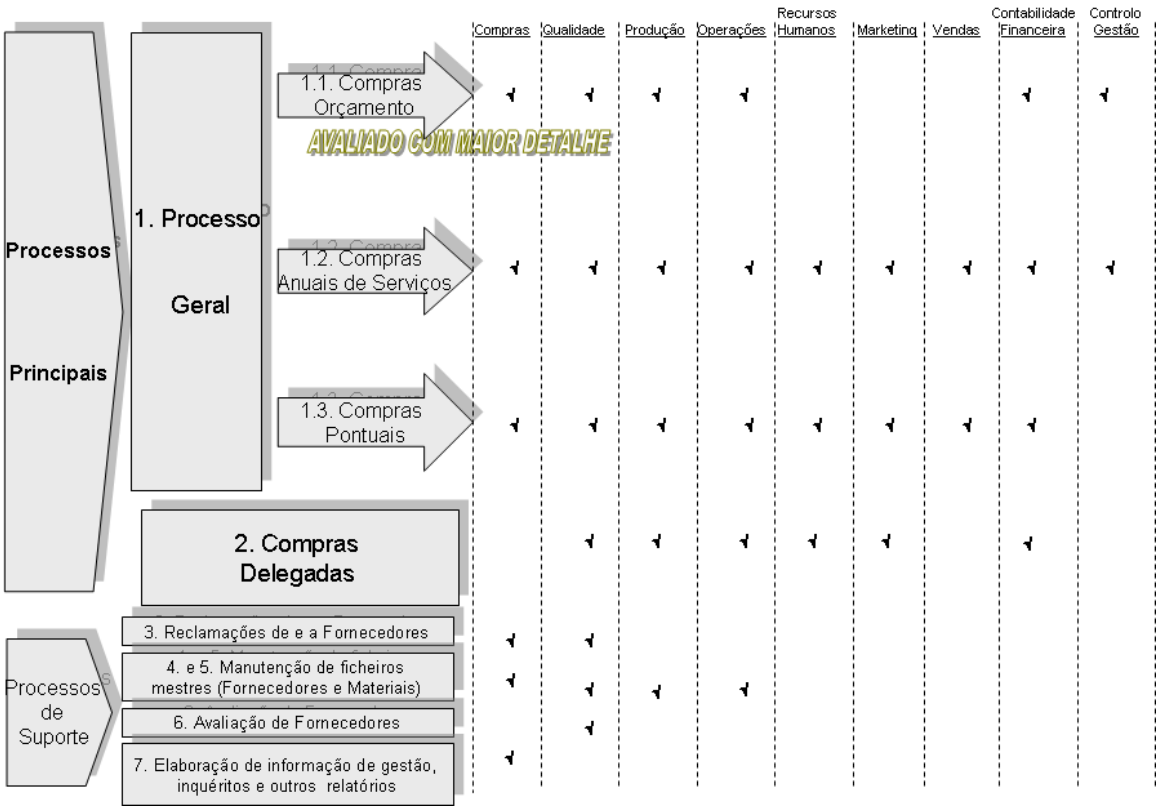


Figura 16: Enquadramento dos processos de Compras na Organização (**Fonte**: Produção Própria)

Conforme se pode verificar na figura 16, os processos de compras estão relacionados com diferentes áreas da empresa. No que diz respeito às compras orçamento verificamos que as áreas envolvidas para além das Compras são a Qualidade, Produção, Operações, Contabilidade/Financeira e Controlo de Gestão. Estamos a referir-nos a áreas que estão abrangidas por este tipo de compra, ou seja, que fornecem ao Departamento de Compras informação (orçamento em quantidade) dos materiais a adquirir.

As compras anuais de serviços são transversais a todas as áreas, pelo que, todas as áreas intervêm neste processo. Relativamente às compras pontuais, verificamos que apenas o Controlo de Gestão não recorre a este tipo de compras, todas as restantes áreas efectuam compras pontuais ao longo do ano. As compras delegadas, tal como o próprio nome indica são compras efectuadas fora do Departamento de Compras, pelo que esta área não está contemplada, assim como, a área de Vendas e de Controlo de Gestão.

As reclamações de e a fornecedores só podem ser efectuadas por duas áreas, a de compras e a da qualidade. A manutenção dos ficheiros mestres de fornecedores e de materiais, também se encontra restringido a quatro áreas, compras, qualidade, produção e operações, isto porque, são as áreas que intervêm no processo de criação/alteração de dados mestre de fornecedores e materiais.

A avaliação de fornecedores e a elaboração de informação de gestão, inquéritos e outros relatórios são exclusivos da área de compras.

5.2.1.3. Estabelecer uma linguagem comum

A nossa análise está focalizada nos processos desenvolvidos no Departamento de Compras, ou seja, aqueles designados como Processo Principal, referidos no ponto 5.2.1.2.1.1. deste documento.

Para dar resposta ao objectivo deste trabalho – a avaliação dos riscos do negócio que afectam o processo de compras – adoptámos o que se convencionou apelidar de "linguagem comum" no tocante à tipificação dos riscos e que detalharemos abaixo.

O COSO, também refere a utilização de uma linguagem comum, no que diz respeito à classificação dos riscos. Tal como referido no ponto 5.1.2. vamos considerar as três categorias de riscos: de envolvente, do processo e da informação para a tomada de decisão, e que a Figura 17 apresenta esquematicamente.

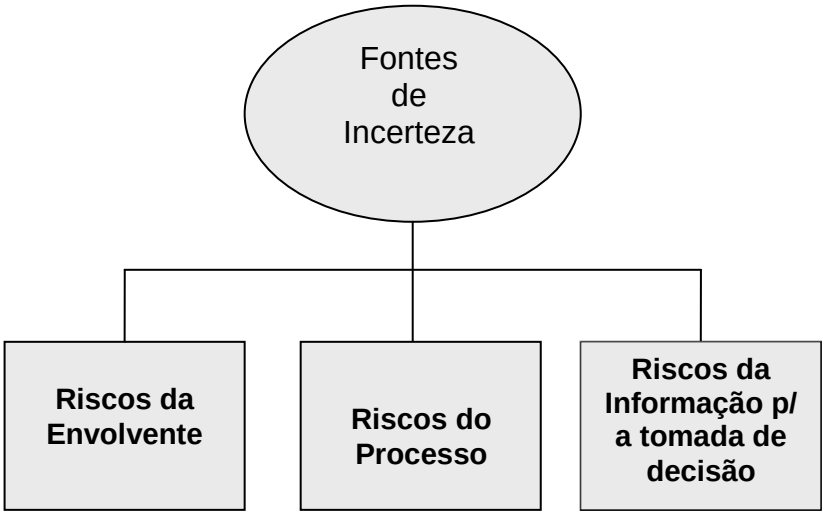


Figura 17: Fontes de Incerteza (**Fonte:** Protiviti, 2006)

Conforme referido no Guide to Enterprise Risk Management (Protiviti, 2006) estes três grupos de riscos estão inter-relacionados. Os riscos da envolvente e do processo que uma empresa enfrenta são originados por realidades do negócio, quer internas, quer externas. O risco relativo à informação para a tomada de decisão é directamente afectado pela eficácia e segurança dos sistemas formais e informais de recolha e de processamento da informação e são estas as três categorias de riscos do negócio que, por sua vez, proporcionam uma ampla base a partir da qual riscos mais específicos podem ser identificados e detalhados.

De seguida fazemos uma breve apresentação dos riscos específicos de cada uma destas categorias de risco de negócio e que vão fazer parte da matriz de risco que vamos apresentar no caso prático. Em anexo será apresentado um manual de ricos de negócio com todos os riscos da matriz utilizada na aplicação prática, incluindo uma breve descrição de cada um deles (Anexo 1).

No que diz respeito ao Risco do Meio Envolvente, consideramos os seguintes riscos específicos: Disponibilidade de Capital, Perda Catastrófica, Concorrência, Mercados Financeiros, Indústria, Legal, Normativo, Sensibilidade, Relações com Accionistas e Político.

Relativamente ao Risco do Processo, o mesmo é ainda subdividido em cinco subgrupos, Risco Operacional, Risco de Autoridade e Risco Tecnológico/ Processamento da Informação, Risco de Integridade e Risco Financeiro. Por sua vez, cada um destes subgrupos tem riscos específicos associados que passamos a elencar.

No que diz respeito ao Risco Operacional, foram considerados os seguintes riscos específicos: Interrupção do Negócio, Capacidade, Cumprimento Normas e Regulamentos, Satisfação dos Consumidores, Tempo do processo, Eficiência, Ambiental, Saúde e Segurança, Obsolescência, Recursos Humanos, Expectativas Performance, Desenvolvimento do produto, Falha do Produto/Fornecimento e Perda de Valor das Marcas.

Quanto ao risco de autoridade, foram-lhe associados os seguintes riscos específicos: Autorizações, Facilidade de mudança, Comunicação, Liderança, Subcontratação e Incentivos Performance.

Relativamente ao Risco Tecnológico/Processamento de Informação, os riscos específicos são: Acessos, Disponibilidade, Integridade dos Sistemas de Informação, Infra-estruturas e Relevância da Informação.

Fazem parte do Risco de Integridade os seguintes riscos específicos: Fraude do Colaborador, Actos Ilegais, Fraude da Gestão, Reputação e Uso não Autorizado.

O Risco Financeiro tem os seguintes riscos específicos associados: Crédito-Colateral, Crédito-Concentração, Crédito-Escassez, Liquidiez-Cash Flow, Liquidez-Concentração, Preço Câmbio, Preço-Capitais Próprios, Preço-Instrumentos Financeiros e Preço-Taxa de Juro.

O Risco de Informação para a tomada de decisão, também se subdivide em três subgrupos: Risco Operacional, Risco Financeiro e Risco Estratégico.

No que diz respeito ao Risco Operacional, consideramos os seguintes riscos específicos: Alinhamento, Contratos/Compromissos, Avaliaçação da Performance (operacional), Preço e Reporte Normativo Operacional.

O Risco Financeiro tem os seguintes riscos especificos associados: Informação Contabilística, Orçamento, .Avaliação da Informação de Gestão, Avaliação de Investimentos, Fundo de Pensões, Reporte Normativo (Financeiro) e Impostos.

Quanto ao Risco Estratégico foram considerados os seguintes riscos específicos: Portefólio do Negócio, Avaliação do Ambiente de Negócio, Ciclo de Vida, Organização da Empresa, Avaliação da Performance (Estratégica), Planeamento, Alocação de Recursos e a valorização. A figura 18 apresenta em quadro os diferentes tipos de riscos enumerados e que vão servir para a elaboração das nossas matrizes de risco. Na figura já consta a atribuição de um número a cada risco específico. Este número vai ser o que identificará cada risco específico nas nossas tarefas subsequentes.

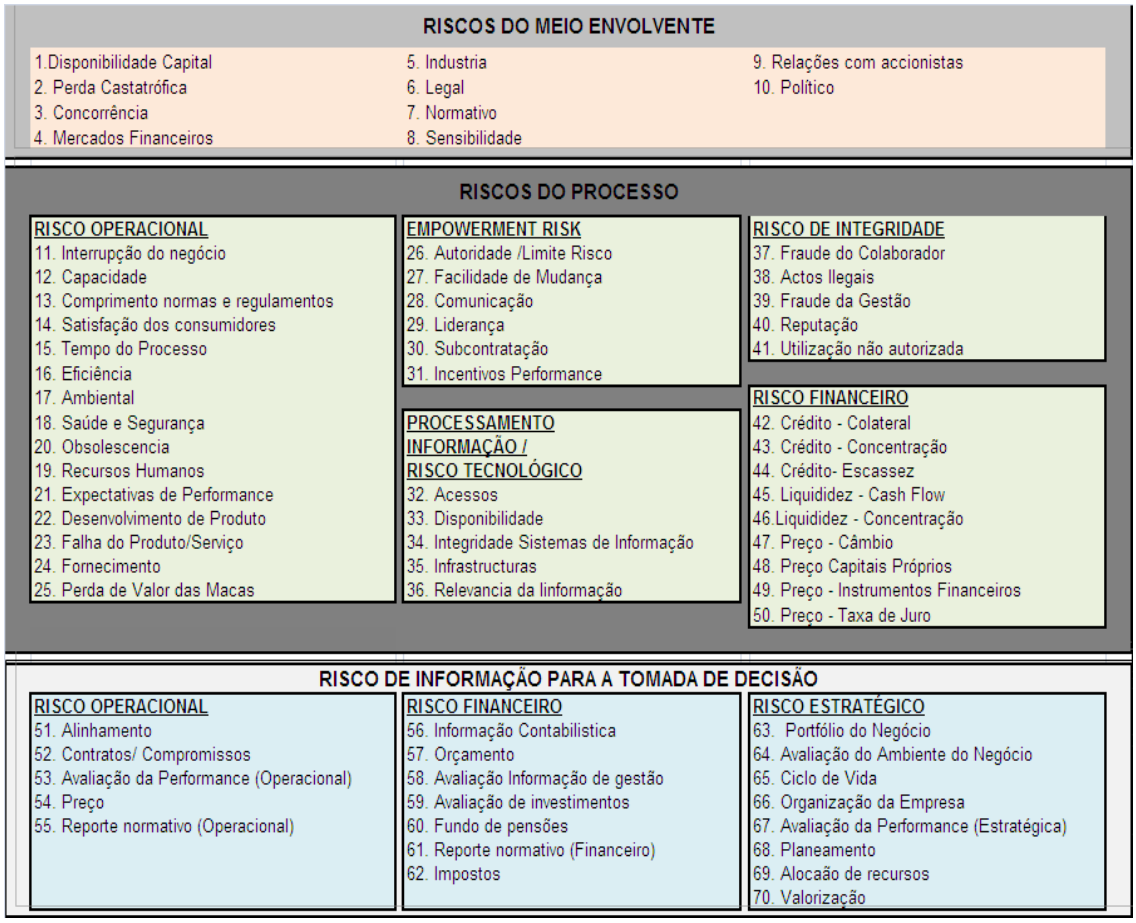


Figura 18 . Matriz de Riscos de Negócio (**Fonte:** Adaptada da Business Risk Model – PricewaterhouseCoopers, 2002)

Para além de ser importante um forte conhecimento dos processos de negócio, é fundamental a linguagem comum proporcionada pelo mapa de riscos, para que as organizações estejam mais preparadas para atingir os objectivos estratégicos (Castanheira e Rodrigues, 2006b).

5.2.2. Processo de Avaliação dos Riscos

O processo de avaliação dos riscos envolve três fases: i) identificação do risco, ii) a análise do risco e iii) a avaliação do risco, conforme referido no ponto 5.1.2. Modelo e fases de aplicação.

5.2.2.1. Identificação dos riscos - Risco Absoluto

O segundo passo do processo de gestão de risco consiste na identificação dos riscos a serem geridos. De acordo com a norma AS/NZS 4360:2004 é fundamental que se

faça uma correcta identificação dos riscos, isto porque, os riscos que não foram identificados nesta fase dificilmente serão analisados em fases posteriores. A identificação deve incluir todos os riscos independentemente da existência ou não de controlos. De acordo com Cicco e Fantazzini (2003), uma das técnicas mais utilizadas na identificação dos riscos são as “checklists” (questionários). De salientar que por mais extensos que sejam estes questionários existe uma probabilidade dos mesmos omitirem situações de risco, pelo que, para evitar que situações destas ocorram cada organização (gestor de risco), deverá adaptar o questionário às características e especificidades da sua empresa.

A identificação dos riscos é efectuada com recurso à construção de uma matriz de riscos por processos (Anexo 2), classificados de acordo com o impacto e probabilidade de ocorrência dos mesmos. Uma matriz de riscos é um documento que apresenta de forma gráfica os riscos de uma organização. Conforme referido acima esta matriz obtêm-se tendo em consideração a valorização do risco do negócio, baseada na análise que foi feita aos processos de negócio e tendo em consideração o impacto e a probabilidade dos riscos identificados. Contudo, esta avaliação também pode ser suportada com base nos resultados de determinados indicadores relacionados com os principais riscos identificados do negócio.

De acordo com Moro (1999:73), “as fases de elaboração do mapa de riscos são as seguintes: Identificação dos riscos do negócio enfrentados por cada um dos processos de actividade; Quantificação e hierarquização do risco; Incorporação das análises realizadas no modelo do mapa de riscos”, pelo que vem de encontro à metodologia seguida no caso prático.

Entende-se por Risco inerente/absoluto, o risco que existe para qualquer entidade, na ausência de quaisquer acções que a Gestão venha a tomar, com vista a alterar, quer a probabilidade de ocorrência do mesmo, quer o respectivo impacto.

Os riscos foram classificados de acordo com o nível de impacto e a probabilidade. O resultado desta classificação está apresentado na matriz de risco inerente, conforme se pode ver na figura 19.

O mapa a seguir apresentado reúne os riscos de negócio identificados e que foram considerados mais significativos e sobre os quais incidiu este trabalho. Salientamos, mais uma vez, que os riscos aqui apontados correspondem à percepção que a Auditoria Interna teve do risco absoluto/inerente que afecta os processos referidos no

ponto 5.2.1.2. desta dissertação, ou seja, antes de identificados os controlos e realizada a análise à qualidade desses mesmos controlos.

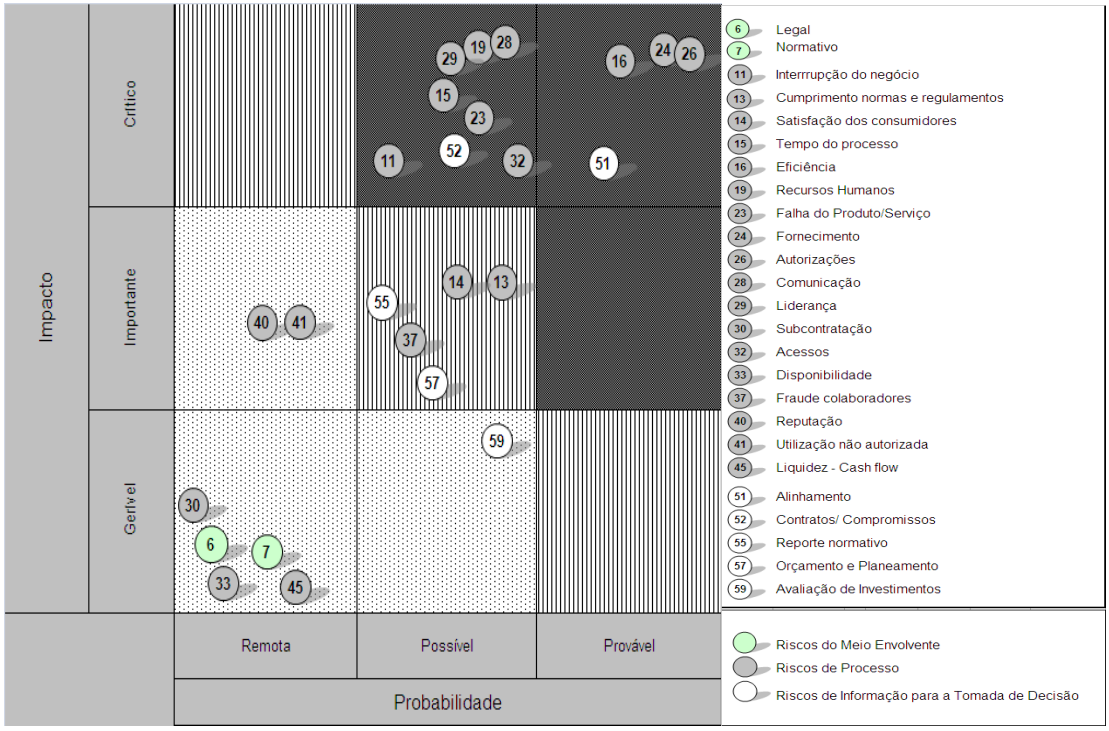
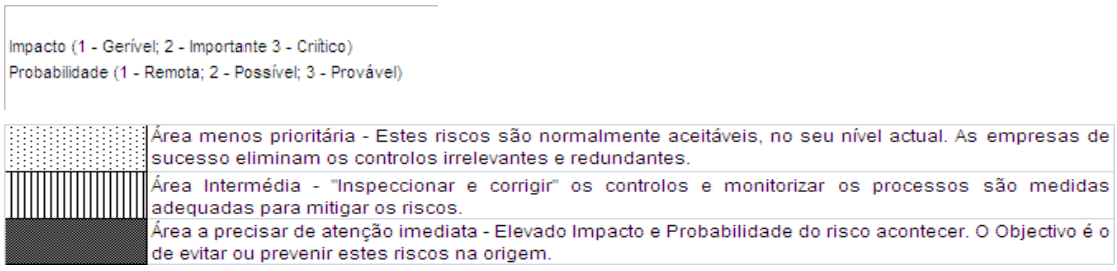


Figura 19: Matriz de Risco Inerente dos Processos de Compras (**Fonte: Adaptada** de Protiviti, 2006)

Legenda:



Face à classificação dos riscos em cada um dos sub-processos avaliados na Área de Compras construímos na figura 20, um ***ranking de ocorrência*** dos cinco riscos considerados mais importantes, ou seja, aqueles em que o produto entre o grau de impacto no negócio (1 – Gerível, 2 – Importante e 3 - Crítico) e a probabilidade de ocorrência (1 – Remota, 2 – Possível e 3 – Provável) é maior do que 3 no processo analisado.

TOP 5 Risco Absoluto Riscos com classificação igual ou superior a Impacto "Importante" e Ocorrência "Possível" [Risco Abs. - Impacto x Probabilidade >3]	
1	24 Fornecimento - Risco de não existir no mercado o material/serviço com o preço/qualidade desejado pela Unidade de Negócio ou de o fornecedor não ter capacidade para satisfazer as necessidades da empresa
	26- Risco de Autoridade -Risco das acções serem executadas por quem não tem autoridade e de descurar as acções que lhe estão atribuídas. Este risco ocorre quando colaboradores da empresa excedem as fronteiras de delegação ou autoridade, ocasionando situações de actos não autorizados, ilegais, não éticos ou assumem riscos do negócio não autorizados e inaceitáveis.
2	16. Efficiência - Risco de ineficiência na satisfação das necessidades dos clientes internos
3	51 Alinhamento - Risco das medidas de performance dos processos do negócio não estarem alinhadas com a estratégia e objectivos da empresa.
4	28. Comunicação - Risco de a comunicação horizontal e vertical não ser eficiente resultando em mensagens inconsistentes com os objectivos propostos e a estratégia da Organização

Figura 20: Tabela dos riscos mais importantes (Relativas aos cinco riscos inerentes mais significativos) (Impacto> 3) (**Fonte:** Produção Própria)

Desta forma, a leitura que podemos fazer da figura 20 é a seguinte:

Por exemplo, o risco de fornecimento - Risco de rupturas ou custos elevados devido a insuficiências no fornecimento de materiais de embalagem para as operações da Empresa, pode levar à incapacidade da Empresa satisfazer as necessidades dos clientes a preços competitivos, nas datas necessárias com a qualidade esperada – posicionou-se em primeiro lugar dentro da totalidade dos riscos do processo, como sendo o mais importante, exequo com o risco de Autoridade. Foram os dois riscos que obtiveram pontuações mais elevadas, logo os mais preocupantes e os que requerem uma atenção especial por parte da gestão.

Conforme já foi referido, os riscos foram identificados e avaliados de acordo com os processos que foram considerados na área de Compras. Na figura 21 apresentamos o processo analisado com maior detalhe:

Processos / Riscos	
1.1. Compras Orçamento	1.1.2. Selecção do fornecedor e validação das condições
	1.1.4. Criação do Acordo de Fornecimento

Figura 21: Tabela do Processo Auditado (**Fonte:** Produção Própria)

O sub-processo “Selecção do fornecedor e validação das condições” aparece como sendo aquele que apresenta maior número de riscos significativos.

Nas matrizes de dupla entrada dos processos disponibilizadas em anexo (Anexo 3), pode ser feita essa leitura da relação entre os riscos identificados e o processo analisado e a respectiva pontuação. A seguir apresentamos, a título exemplificativo, um excerto de uma dessas matrizes.

Processos / Riscos		6. Legal	7. Normativo	11. Interrupção do negócio	13. Cumprimento normas e regulamentos	14. Satisfação do Consumidor	15. Tempo do Processo	16. Eficiência
1.1. Compras Orçamento	1.1.2. Selecção do fornecedor e validação das condições	2	1	6	4	4	6	9
	1.1.4. Criação do Acordo de Fornecimento	1	1	6	1		6	4
	Nº Ocorrências	2	2	2	2	1	2	2
	Nº Ocorrências [Risco Abs. >3]	0	0	2	1	1	2	2

Figura 22: Excerto da Matriz de Risco Inerente dos Processos Auditados (**Fonte:** Produção Própria)

Encontra-se em anexo (Anexo 2) a matriz de risco inerente dos sub-processos analisados, que materializa a 2ª fase do modelo de gestão de risco, ou seja é feita a identificação e a avaliação dos riscos absolutos. De seguida é efectuado o mapeamento dos riscos e respectiva representação gráfica (3ªfase), conforme se apresenta no documento em anexo (Anexo 3).

5.2.2.2. Análise dos riscos

A análise de riscos tem como finalidade perceber qual o nível de risco e a sua natureza. Esta análise fornece informações que determinam a necessidade ou não de tratar os riscos identificados, bem como, permite identificar as estratégias de tratamento mais adequadas e com custos mais reduzidos.

De acordo com a norma AS/NZS 4360:2004 a análise dos riscos tem em consideração as fontes de risco, as suas consequências quer sejam positivas quer sejam negativas e ainda a probabilidade de que as mesmas ocorram. A mesma norma refere que pode ser feita uma análise preliminar, de modo a agregar riscos semelhantes ou riscos com baixo impacto, excluindo-os de um trabalho mais detalhado e aprofundado.

Tendo como referência os riscos identificados apresentados em anexo (anexo 3), procedemos à identificação e avaliação dos controlos executados na área de Compras com o objectivo de aferir o risco residual à data de realização deste trabalho

e propor medidas de controlo que permitam a sua redução. De referir que o risco residual, poderá sofrer alterações, caso se definam e implementem novas medidas eficazes na mitigação dos riscos identificados.

Passamos à análise dos controlos do processo considerado para efeito deste trabalho, isto é, o Grupo de Material de Embalagem.

Para cada um dos sub-processos foi construída uma matriz de análise dos riscos e controlos. Estas matrizes sintetizam o trabalho de análise realizado e que se pode resumir nos seguintes pontos:

- Identificação dos processos auditados (Estes processos são elencados na tabela da figura 22);
- Identificação do risco absoluto destes processos, previamente analisado em conjunto com a área auditada, conforme descrito no ponto 5.2.2.1. Análise e avaliação dos controlos que compreendeu os seguintes passos:
    - Identificação dos controlos aplicados aos processos auditados. Incluem-se neste conceito os procedimentos de controlo previstos no Manual de Procedimentos de Controlo Interno da Empresa, Procedimentos de Controlo previstos nas normas da Qualidade e outros controlos da área;
    - Caracterização dos controlos de acordo com parâmetros
    - Selecção de amostras de processos e execução de testes de verificação da aplicação dos controlos identificados - Simulados;
    - Documentação dos resultados dos testes e avaliação da qualidade dos controlos (Bom, Mau ou Insuficiente);
- A classificação dos riscos foi revista com base nos resultados da avaliação dos controlos, da qual resulta a matriz de risco residual que apresentaremos mais adiante.

De referir que os controlos podem ter diferentes classificações, nomeadamente, manuais ou automáticos; preventivos, detectivos ou correctivos; primários ou secundários.

Os controlos manuais dependem predominantemente da execução manual de uma ou mais pessoas.

Os controlos automáticos estão embebidos em programas informáticos ou aplicações de tecnologias de informação e executam um passo ou previnem uma transacção de ocorrer sem uma decisão manual ou iteração.

Existem ainda controlos manuais dependentes de sistemas de informação, isto é, controlos que são manuais mas que se baseiam em informação retirada dos sistemas de informação.

Controlos preventivos, manuais ou automáticos, são desenhados para prevenir erros ou omissões de ocorrer e são geralmente posicionados junto à fonte do risco dentro do processo de negócio.

Controlos detectivos são processos, manuais ou automáticos, que são desenhados para detectar ou corrigir um erro ou uma omissão, antes da concretização do objectivo.

Controlos correctivos são similares aos controlos detectivos mas tem o objectivo específico de corrigir o erro detectado.

Controlos primários são controlos que são especialmente críticos na mitigação do risco.

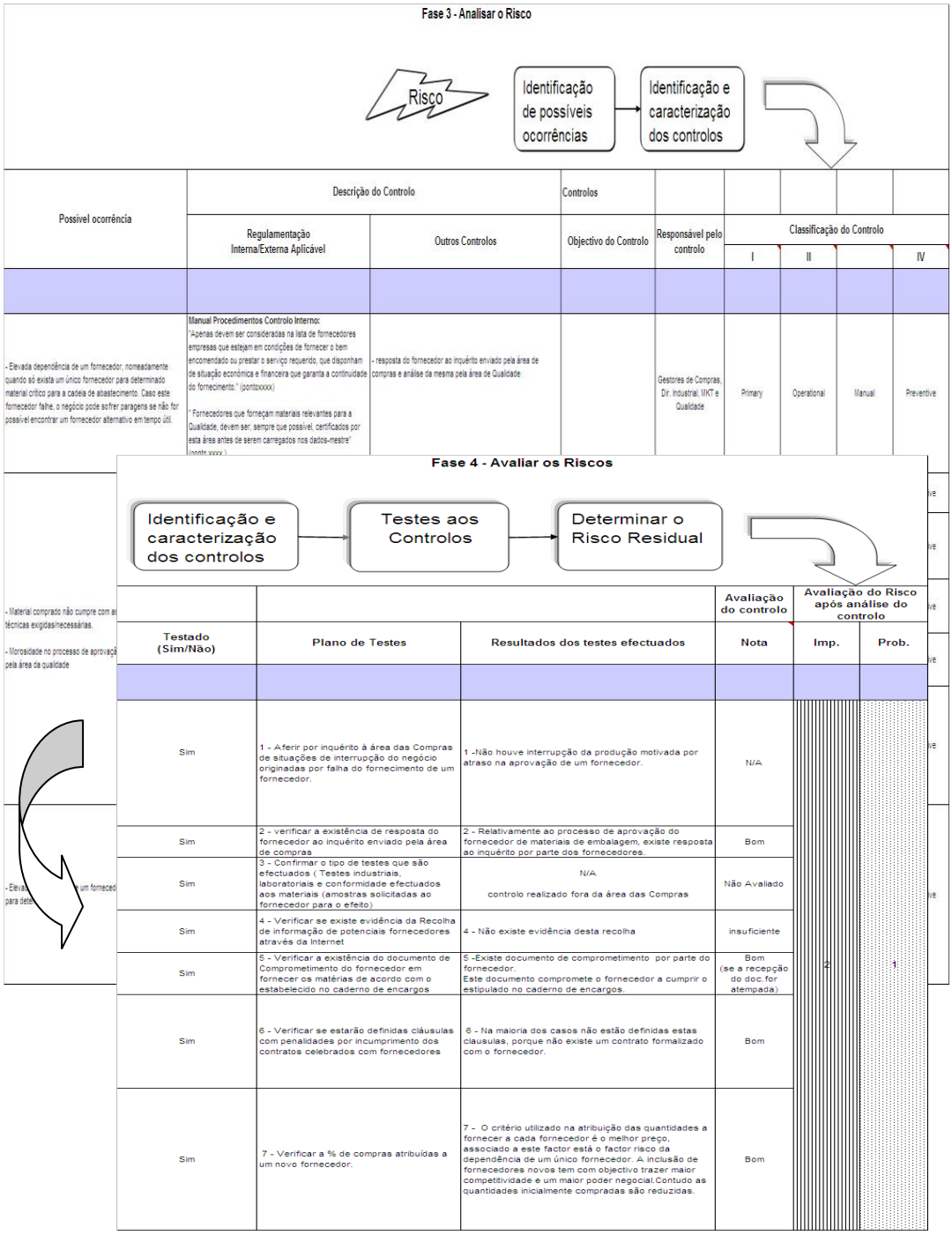
Controlos secundários são importantes para a mitigação do risco mas não são considerados críticos pela Gestão e pelos donos dos processos. Apesar destes controlos serem importantes existem controlos alternativos que garantem a concretização dos objectivos.

Os controlos podem ainda ser operacionais, de cumprimento ou financeiros. A maior parte dos controlos internos servem para cumprir mais do que um objectivo. Em determinadas situações, os controlos implementados para atingir objectivos operacionais ou de cumprimento, também podem satisfazer objectivos relacionados com a informação financeira.

Os controlos operacionais referem-se à eficácia e eficiência das operações e à salvaguarda dos recursos disponíveis. Os controlos de cumprimento estão relacionados com o cumprimento de leis e regulamentos aplicáveis na organização e os controlos financeiros são os que dizem respeito à informação financeira.

Os mapas de análise dos riscos e controlos foram preparados por Sub-processo e estão disponibilizadas em anexo para consulta (Anexo 4).

A Figura 23 representa, a título exemplificativo, um excerto de uma dessas matrizes.



Possível ocorrência	Descrição do Controlo		Controlos					
	Regulamentação Interna/Externa Aplicável	Outros Controlos	Objectivo do Controlo	Responsável pelo controlo	Classificação do Controlo			
					I	II		IV
- Elevada dependência de um fornecedor, nomeadamente quando só exista um único fornecedor para determinado material crítico para a cadeia de abastecimento. Caso este fornecedor falhe, o negócio pode sofrer paragens se não for possível encontrar um fornecedor alternativo em tempo útil.	Manual Procedimentos Controlo Interno: "Apenas devem ser consideradas na lista de fornecedores empresas que estejam em condições de fornecer o bem encomendado ou prestar o serviço requerido, que disponham de situação económica e financeira que garanta a continuidade do fornecimento." (pontoxxxx) * Fornecedores que forneçam materiais relevantes para a Qualidade, devem ser, sempre que possível, certificados por esta área antes de serem carregados nos dados-mestre" (ponto xxxx.)	- resposta do fornecedor ao inquérito enviado pela área de compras e análise da mesma pela área de Qualidade		Gestores de Compras, Dir. Industrial, MKT e Qualidade	Primary	Operational	Manual	Preventive

			Avaliação do controlo	Avaliação do Risco após análise do controlo	
Testado (Sim/Não)	Plano de Testes	Resultados dos testes efectuados	Nota	Imp.	Prob.
Sim	1 - Aferir por inquérito à área das Compras de situações de interrupção do negócio originadas por falha do fornecimento de um fornecedor.	1 -Não houve interrupção da produção motivada por atraso na aprovação de um fornecedor.	N/A	2	1
Sim	2 - verificar a existência de resposta do fornecedor ao inquérito enviado pela área de compras	2 - Relativamente ao processo de aprovação do fornecedor de materiais de embalagem, existe resposta ao inquérito por parte dos fornecedores.	Bom		
Sim	3 - Confirmar o tipo de testes que são efectuados (Testes industriais, laboratoriais e conformidade efectuados aos materiais (amostras solicitadas ao fornecedor para o efeito)	N/A controlo realizado fora da área das Compras	Não Avaliado		
Sim	4 - Verificar se existe evidência da Recolha de informação de potenciais fornecedores através da Internet	4 - Não existe evidência desta recolha	insuficiente		
Sim	5 - Verificar a existência do documento de Comprometimento do fornecedor em fornecer os matérias de acordo com o estabelecido no caderno de encargos	5 -Existe documento de comprometimento por parte do fornecedor. Este documento compromete o fornecedor a cumprir o estipulado no caderno de encargos.	Bom (se a recepção do doc.for atempada)		
Sim	6 - Verificar se estarão definidas cláusulas com penalidades por incumprimento dos contratos celebrados com fornecedores	6 - Na maioria dos casos não estão definidas estas clausulas, porque não existe um contrato formalizado com o fornecedor.	Bom		
Sim	7 - Verificar a % de compras atribuídas a um novo fornecedor.	7 - O critério utilizado na atribuição das quantidades a fornecer a cada fornecedor é o melhor preço, associado a este factor está o factor risco da dependência de um único fornecedor. A inclusão de fornecedores novos tem com objectivo trazer maior competitividade e um maior poder negocial.Contudo as quantidades inicialmente compradas são reduzidas.	Bom		

Figura 23: Exemplo de Matriz de Análise dos Controlos ao Processo Analisado (excerto) (**Fonte:** Produção própria)

Este mapa de análise de riscos e controlo, serve para apresentar de forma clara e precisa toda a informação relacionada, quer com a análise dos riscos, quer com a identificação e avaliação dos controlos do processo.

Depois de identificados e avaliados os riscos absolutos dos diferentes sub-processos em análise, passamos às fases de análise dos riscos, identificação e avaliação dos controlos.

Este mapa não é mais do que um documento que reúne toda a informação necessária ao desenvolvimento e suporte das fases 3 e 4 (análise e avaliação dos riscos) do modelo de gestão de risco adoptado na elaboração deste trabalho.

Depois de identificados e avaliados os riscos absolutos, elabora-se o mapa acima referido com a informação necessária, ou seja, identificamos e descrevemos as possíveis ocorrências (para cada risco identificado), identificamos e descrevemos os controlos diferenciando os que estão suportados em regulamentação interna e ou externa, o objectivo dos controlos, o responsável pelo mesmo e classificamos os controlos de acordo com a sua natureza, isto é, se são controlos primários ou secundários, operacionais, de cumprimento ou financeiro, se são manuais ou baseados em sistemas de informação, se são controlos preventivos, detectivos ou correctivos.

De seguida, passa-se à fase dos testes de conformidade. Com base no programa de testes elaborado, vamos verificar se os controlos existentes são ou não eficazes na mitigação dos riscos identificados. Com base na avaliação dos controlos, vamos reclassificar os riscos, determinando-se assim a matriz dos riscos residuais.

5.2.2.3. Avaliar os riscos

De acordo com a Norma AS/NZS 4360:2004, a avaliação dos riscos tem como finalidade a tomada de decisões, suportada nos resultados da análise de riscos, sobre quais precisam de ser tratados e sobre a prioridade de tratamento.

Esta fase corresponde ao quarto passo do processo de gestão de risco (anexo 4), sendo a fase em que se chega à matriz de risco que de seguida deverá ser gerido (anexo 5).

Depois de analisados e avaliados os controlos existentes no processo auditado, foi possível rever a classificação atribuída aos riscos identificados e apurado desta forma o risco residual dos processos.

A avaliação final é resultado da maior classificação atribuída a um risco, por exemplo o sub-processo 1.1.2 no risco Eficiência tem 9 e o sub-processo 1.1.4 no mesmo risco tem 4, a avaliação final do risco do processo é 9.

Se estivéssemos a avaliar mais do que um processo, já teríamos que fazer a ponderação dos processos, por exemplo tendo em conta o peso de cada um no total das compras.

Risco residual, como vimos, é aquele que permanece depois de implementados os controlos e medidas de redução do risco. O objectivo óptimo será que o risco residual tenda para zero.

Partindo da matriz inicialmente apresentada com o Risco Inerente atribuído a cada um dos processos auditados (figura 19), chegámos à Matriz de Risco Residual que é apresentada na figura 24.

Neste caso em concreto, estamos a referir-nos ao risco residual à data de elaboração deste trabalho, ou seja, tendo em consideração os controlos existentes e qualidade desses mesmos controlos na mitigação dos riscos identificados. Contudo, este risco poderá ainda ser reduzido, caso sejam implementadas as sugestões/recomendações da Auditoria Interna e ou outras medidas que a área considere adequadas na mitigação quer dos riscos identificados, quer de outros que possam entretanto surgir.

Na aplicação prática do modelo de gestão de risco apresentada neste trabalho, não iremos analisar a fase do tratamento de riscos, nem a fase da monitorização/revisão, pelo que, não nos poderemos pronunciar, sobre a possibilidade deste risco residual ser alterado em virtude das recomendações efectuadas pela Auditoria Interna, ou mesmo, através de novas medidas de controlo que tenham sido implementadas por iniciativa da própria área auditada.

Esta questão poderá ser abordada e aprofundada num trabalho futuro sobre o tema em análise.

Face à avaliação realizada sobre os controlos, a lista dos principais riscos inicialmente calculada tendo como referência o risco absoluto sofreu naturalmente algumas mudanças tendo mesmo ocorrido a saída de alguns riscos dessa lista e a entrada de outros que inicialmente não se consideravam tão relevantes.

Depois de identificados, analisados e avaliados os controlos existentes para os riscos objecto de análise, o que corresponde à 4ª fase do modelo de gestão de Risco (Anexo 4), determinamos o risco residual que apresentamos através da Matriz de Risco Residual (Figura 24).

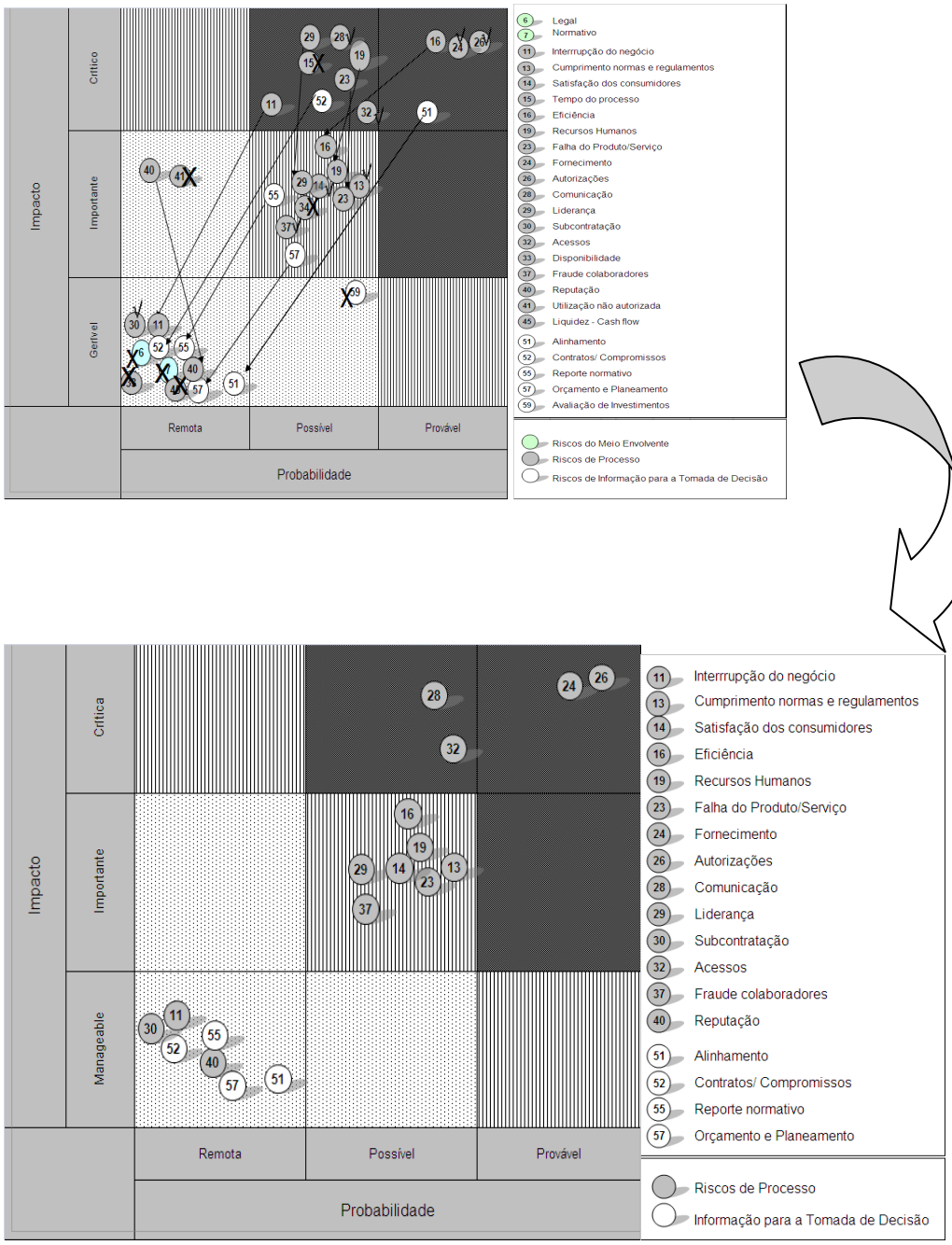


Figura 24: Matriz de Risco Residual dos Processos Auditados (**Fonte:** Adaptado de Protiviti –, 2006)

Identificados os riscos residuais, o passo seguinte diz respeito ao tratamento dos riscos residuais, ou seja, definir possíveis medidas que possam ser implementadas de modo a mitigar o risco residual.

Apresentamos em anexo (Anexo 6) um exemplo de matriz de tratamento de risco associado a este trabalho e que representa a 5ª fase do modelo de Gestão de Risco apresentado.

Podemos por conseguinte considerar que esta lista que a seguir apresentamos, Figura 25, representa os riscos que na nossa perspectiva merecem uma atenção prioritária da Gestão e que deverão por isso mesmo levar à introdução de melhorias ao nível dos controlos e de mecanismos de gestão de forma que sejam tratados e reduzidos para os níveis desejados (mitigação de riscos).

TOP 5 Risco Residual Riscos com classificação igual ou superior a Impacto "Importante" e Ocorrência "Possível" [Risco Abs. - Impacto x Probabilidade >3]	
1	**26. Risco de Autoridade** - Risco de dos colaboradores realizarem tarefas que não era suposto ou não realizarem as tarefas que lhes estavam atribuídas.
2	**24. fornecimento** - Risco de não existir no mercado o material/serviço com o preço/qualidade desejado pela Unidade de Negócio ou de o fornecedor não ter capacidade para satisfazer as necessidades da empresa.
3	**28. Comunicação** - Risco de a comunicação horizontal e vertical não ser eficiente resultando em mensagens inconsistentes com os objectivos propostos e a estratégia da Organização
4	**32. Acessos** - O risco de acesso inclui o risco que o acesso à informação (dados ou programas) seja inadequadamente concedido ou recusado. Significando a concessão de acessos a informação confidencial a pessoas não autorizadas ou incorrectamente autorizadas.
5	**16. Eficiência** - Risco de ineficiência na satisfação das necessidades dos clientes internos

Figura 25: Tabela de frequência das ocorrências (Relativas aos riscos residuais mais significativos, com impacto> 3) (**Fonte:** Produção própria)

A matriz representada na figura 24 e a respectiva tabela com os riscos mais significativos (figura 25), espelham aquilo, que fruto da análise seguida aplicando a metodologia de gestão de risco, serão os riscos que afectam o processo de compras, e mais concretamente a actividade desenvolvida no Departamento de Compras.

No sentido de se completar esta visão transversal do processo de Compras, esta análise deverá ser estendida às restantes áreas onde o mesmo ocorre.

Estas matrizes deverão ser entendidas como uma ferramenta de trabalho que permitirá à Empresa, e neste caso aos responsáveis pelo processo analisado, facilitar a sua actividade de gestão, focalizando-se em primeiro lugar na resolução daqueles que são os riscos mais importantes e que mais poderão condicionar os objectivos e a estratégia da Empresa.

No ponto 5.2.3. Tratar os riscos, apresentamos uma proposta de recomendações que na nossa perspectiva poderão melhorar os níveis de controlo e introduzir maior eficiência nos processos de forma a reduzir os níveis de riscos.

5.2.3. Tratar os riscos

Após se conhecer quais os riscos que devem ser geridos, passamos ao passo 5 que consiste na apresentação das recomendações para gerir esses riscos.

De acordo com a norma AS/NZS 4360:2004, "o tratamento de riscos envolve a identificação das diferentes opções para tratar os riscos, a análise e a avaliação dessas opções e a preparação e implementação de planos de acção".

Deste modo apresentamos possíveis recomendações para o TOP 5 dos riscos identificados.

Processo: Compras - Processo Geral - Selecção do Fornecedor

Risco: 26. Risco de Autoridade

Falha de Controlo: Processos de compra em que não existe qualquer documento que justifique a escolha do fornecedor, ou os critérios que estiveram na base dessa decisão, bem como, não existe evidência da aprovação.

Recomendação: Entendemos que deve sempre existir um documento justificativo da escolha do fornecedor e evidência da sua aprovação, de modo a garantir que a escolha foi efectuada por pessoa autorizada e a quem está atribuída essa competência.

Sugerimos que seja definido um documento modelo obrigatório que contenha os motivos que justifiquem a escolha do fornecedor, documento este que deverá estar arquivado juntamente com o processo de compras. Estes mapas deverão apresentar evidência de aprovação de acordo com os níveis de delegação definidos no documento interno.

Risco: 24. Fornecimento

Falha de Controlo: A informação solicitada a fornecedores de materiais em que o risco de fornecimento é elevado que permita avaliar a sua capacidade financeira e situação económica não parece ser suficiente podendo conduzir a risco de

fornecimento, falha do produto ou eficiência no caso de o fornecedor enfrentar problemas financeiros/económicos significativos.

Recomendação: Na admissão de um novo fornecedor nacional, sugerimos que se verifique se a firma em causa se encontra na Lista de Devedores ao Fisco disponibilizada no site das Finanças.

No caso de fornecedores em que o montante em negociação assume proporções significativas (de acordo com limite a definir pelo Departamento de Compras) ou para materiais críticos, e se perspectivem períodos de fornecimento longos (por exemplo 1 ano), deverá ser ponderada a recolha de informação económico-financeira do fornecedor por recurso a entidades especializadas que fornecem este tipo de informação (ex: Dun & Bradstreet e outras entidades).

Risco: 28. Comunicação

Falha de Controlo: Solicitações de cotação efectuadas ao mesmo fornecedor com os materiais repartidos por empresa do grupo. Esta situação leva a que o fornecedor não tenha uma visão consolidada dos materiais e quantidades solicitados para todo o Grupo podendo levar a uma perda de vantagem negocial. Nestas situações o comprador solicita ao fornecedor que veja para as propostas de um modo global.

Recomendação: Sugerimos que seja desenvolvida uma ferramenta que permita que uma solicitação de cotação reúna todas as requisições de compra do mesmo material ignorando os campos Empresa permitindo assim que o fornecedor possa ter o resumo total da quantidade encomendada pelo Grupo.

Riscos: 32. Acessos

O Risco de Acessos não foi avaliado por ser um risco cujos controlos estão suportados sobretudo na segurança do sistema de informação, pelo que optamos por manter a pontuação atribuída ao risco absoluto.

Este risco ficou fora do âmbito deste trabalho, uma vez que se trata de um trabalho específico de auditoria informática, sendo necessário recorrer a profissionais especializados, nomeadamente, auditores informáticos. A análise do risco de Acessos é uma das limitações deste trabalho. Contudo, poderá ser desenvolvido no âmbito de trabalhos futuros.

Riscos: 16. Eficiência

Falha de Controlo: As áreas operacionais não enviam para o Departamento de Compras a informação relativa aos orçamentos atempadamente, ou quando chega é posteriormente alterada, o que pode pôr em causa a recepção de materiais e por conseguinte a satisfação das necessidades dos clientes. Por outro lado, verifica-se situações em que o processo de aprovação de fornecedores é moroso. Ambas as situações atrás referenciadas podem provocar atrasos nas negociações, podendo originar uma perda de oportunidade negocial.

Recomendação: O Departamento de Compras deverá definir juntamente com as Áreas Operacionais um calendário para a recepção de toda a informação necessária, de modo a evitar atrasos e desta forma comprometer o poder negocial, bem como, deverá ser definida uma equipa de trabalho com todos os intervenientes no processo de aprovação de fornecedores com o intuito de se definirem limites temporais razoáveis de intervenção de cada área por tipo de material.

5.2.4. Ficha de análise de riscos e controlos

Apresentamos na Figura 26 um exemplo de uma ficha de Riscos e Controlos que poderá ser utilizada, cujo objectivo é resumir num documento toda as análises e avaliações dos riscos e controlos, bem como, identificar as falhas de controlo (por risco), e efectuar as respectivas recomendações.

Esta ficha de risco inicia-se com a Identificação do Risco e o respectivo enquadramento no processo analisado. Tal como referimos acima, é feita uma ficha de risco para cada risco identificado. De seguida, a ficha inclui em termos gráficos a matriz dos riscos absolutos, que resultou da avaliação dos riscos efectuados em cada sub-processo classificando-o quanto à probabilidade de ocorrência e ao seu impacto sem considerar os controlos existentes.

O passo seguinte, na elaboração da ficha, é a identificação e avaliação dos controlos, ou seja, procedemos à identificação dos controlos implementados para mitigar o risco e avaliação do impacto no processo da falha desse controlo e da robustez do controlo face aos testes realizados.

Depois passamos à inscrição, na ficha, da avaliação do risco residual (à data da análise) em cada sub-processo classificando-o quanto à probabilidade de ocorrência e o seu impacto considerando os controlos existentes.

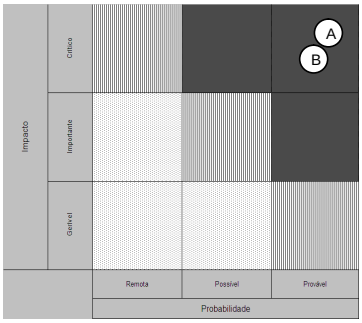
De seguida apresenta-se uma conclusão geral, sobre o risco residual do macro-processo e sobre o risco no âmbito do processo em análise.

Por fim, são identificadas as falhas de controlo e efectuadas as recomendações pela Auditoria Interna que visam reduzir a exposição do processo de compras, sub-processo compras orçamento, ao risco analisado.

Ficha de análise de Riscos e Controlos

Risco: 26 Autorização – O risco das acções serem executadas por quem não tem autoridade e de descurar as acções que lhe são atribuídas.
Este risco ocorre quando colaboradores da empresa excedem as fronteiras de delegação ou autoridade, ocasionando situações de actos não autorizados, ilegais, não éticos ou assumem riscos de negócio não autorizados e inaceitáveis.

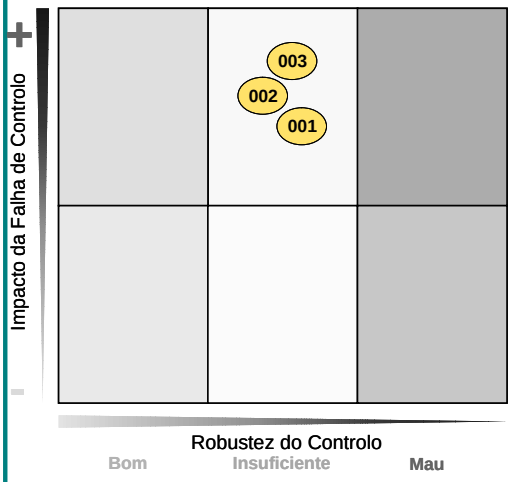
Avaliação do Risco Absoluto (sem considerar os controlos implementados)



Sub-processos

A. Selecção do fornecedor e validação das condições
B. Criação do Acordo de Fornecimento

Mapa de Caracterização dos Controlos



Descrição dos Controlos

A. Selecção do Fornecedor e avaliação das condições

001 – Critérios utilizados na selecção do fornecedor.
002 – Validação das condições

B. Criação do Acordo de Fornecimento

003 – Informação enviada foi validada e aprovada

Figura 26: Ficha de análise de Riscos e Controlos (**Fonte:** Produção Própria)

5.3. Limitações da aplicação prática

A análise do processo de compras de acordo com a metodologia de gestão de risco, adoptada, incidiu sobretudo nas actividades desenvolvidas no Departamento de Compras. Contudo, esta aplicação ficou limitada a um dos sub-processos identificados no Departamento de compras – Compras Orçamento. Este facto limita o estudo efectuado, uma vez que, a avaliação dos riscos não está a ser ponderada por todos os sub-processos onde esse mesmo risco poderá existir. Se tivéssemos em consideração todos os sub-processos, possivelmente existiriam riscos que estariam posicionados de forma diferente.

Não obstante, o processo de compras estar interligado com diferentes áreas da empresa, não foram tidas em consideração quaisquer actividades desenvolvidas nas áreas transversais ao processo e que podem ter impacto (positivo/negativo), na avaliação do risco do Departamento de compras. De salientar também que, a análise de riscos poderia ser efectuada ao nível das actividades. Contudo, dada a complexidade e diversidade de actividades subjacentes a um processo e compras, optámos por focar a análise de risco ao nível de um sub-processo. Por este facto, fica fora do âmbito deste trabalho o levantamento e análise dos processos das áreas transversais ao processo em análise, nomeadamente Controlo de Qualidade, Gestão de Stocks, Armazéns, Produção, entre outras, pelo que, uma opinião sobre o risco residual que afecta todos os restantes processos implica uma análise junto destas áreas operacionais onde os mesmos ocorrem.

Desta forma, para que se possa apresentar uma visão transversal na organização sobre o risco residual é necessário desenvolver uma análise junto das restantes áreas operacionais onde os processos identificados ocorrem.

Só será possível avaliar da adequação dos controlos, depois de analisados todos os processos considerados como fazendo parte do processo de compras e que estão inseridos noutras áreas conforme referido atrás, digamos que será uma das limitações deste estudo.

De salientar o facto de apenas se ter analisado um dos sub-processos (compras orçamento), embora tenham sido identificados mais sub-processos, conforme apresentamos na figura 16.

De referir que o Risco de Acessos não foi avaliado por ser um risco cujos controlos estão suportados sobretudo na segurança do sistema de informação.

Este risco ficou fora do âmbito deste trabalho, uma vez que se trata de um trabalho específico de auditoria informática, sendo necessário recorrer a profissionais especializados, nomeadamente, auditores informáticos.

Relativamente à fase do tratamento de riscos, apenas foram identificadas possíveis acções a desenvolver e efectuadas recomendações que, no entender da Auditoria Interna, ajudam na mitigação dos riscos identificados, isto é, se as medidas forem devidamente implementadas.

Antes de emitir o relatório final, deve ser feito um workshop com o Director da área auditada e com os colaboradores intervenientes no processo para apresentação das conclusões.

De referir, que dada a dimensão do trabalho, não nos foi possível aplicar todas as fases do modelo de gestão de risco, tendo ficado por analisar com detalhe a fase do tratamento de riscos e a fase da monitorização e revisão. Assim, outra das limitações deste estudo é precisamente o facto de não ter sido executado o trabalho de monitorização e Revisão (follow-up) das questões reportadas, nomeadamente no que diz respeito à correcta implementação das recomendações sugeridas pela Auditoria Interna e que corresponde a um passo da Gestão de Risco da Norma Neozelandesa 4360:2004.

Consideramos que as limitações referidas acima poderão ser analisadas e desenvolvidas em trabalhos futuros sobre este tema.

5.4. Análise crítica

Este trabalho trata de um tema muito actual, mas sobre o qual ainda não existe muita informação disponível, nomeadamente ao nível prático. Uma das grandes dificuldades com que nos confrontamos é entender como se podem aplicar estes novos conceitos na nossa actividade profissional, isto é, como é que se pode aplicar na prática um modelo de gestão de risco nos trabalhos executados pela Auditoria Interna.

De acordo com Beja (2004b), há em Portugal, no que respeita à Gestão de Risco, um longo e urgente caminho a percorrer pelas nossas Empresas e pelos nossos Gestores, mas também pelas nossas Escolas e Instituições Profissionais ligadas à Contabilidade e à Gestão.

Deste modo, consideramos que este trabalho poderá servir de guia para a implementação de um modelo de gestão de risco nos trabalhos elaborados pelos Departamentos de Auditoria Interna e, assim, dar um contributo para o caminho que ainda falta percorrer nesta matéria em Portugal.

No entanto, os modelos terão de ser ajustados de acordo com a dimensão e realidade de cada empresa.

> "É forte a convicção de que estamos perante um processo em rápida evolução e em crescimento acentuado, embora ainda num estado embrionário de desenvolvimento teórico e de aplicação prática, em Portugal" (Beja, 2004b:18).

De salientar o aspecto positivo deste trabalho que foi, por um lado, a materialização na prática da norma neozelandesa 4360;2004 e dos conceitos do COSO – ERM num trabalho de Auditoria Interna e, por outro, a visão e o conhecimento que nos permite ter, quer ao nível da área auditada, quer ao nível da empresa como um todo, uma vez que este trabalho é visto de forma transversal, permitindo auxiliar a gestão no cumprimento dos seus objectivos, criando deste modo mais valor para a empresa. Efectivamente, estamos perante uma nova era da Auditoria Interna, que nos permite olhar para o presente e futuro e não apenas para factos passados, passando a centrar a atenção nos riscos, fornecendo informação relevante para a tomada de decisão da Gestão.

Não podemos deixar de salientar que a aplicação deste modelo, tal como é apresentado é um pouco complexo, nomeadamente no que diz respeito aos documentos de suporte (matrizes de risco, avaliação dos controlos, etc.). Contudo, todos estes mapas devem ser ajustados à realidade e dimensão de cada empresa. Aliás, podem ser desenvolvidos outros tipos de mapas, de acordo com as necessidades de cada empresa, desde que se consiga obter e documentar convenientemente a informação suporte do trabalho realizado.

Para que a aplicação de um modelo de gestão de risco tenha sucesso é fundamental que todas as pessoas estejam devidamente informadas sobre a Gestão de Risco Empresarial, de modo, a que haja uma consciencialização de que todos são importantes no processo de Gestão de Risco da sua empresa. Os Auditores Internos devem avaliar até que ponto a gestão de riscos adoptada e aplicada pela empresa é eficaz na mitigação dos riscos do negócio para um nível aceitável, de modo, a que sejam atingidos os objectivos propostos. É importante realçar que nem todas as empresas estão no mesmo

nível de implementação da gestão de riscos, o qual terá impacto no trabalho que será desenvolvido pela Auditoria Interna.

Cada empresa deverá adoptar o seu modelo de gestão de risco e numa primeira fase, a empresa deverá promover acções de formação, nomeadamente, a todos os gestores de topo e intermédios, com o objectivo de os consciencializar para esta temática e incutir a responsabilidade que cada um tem no processo de gestão de risco da empresa.

Trata-se de uma visão integrada dos riscos, isto é, os riscos são analisados de forma transversal à organização, o que proporciona uma melhor avaliação dos riscos e dos controlos implementados na mitigação dos riscos do negócio e na concretização dos objectivos estratégicos e operacionais definidos.

6. CONCLUSÃO

A Auditoria Interna apresenta uma mudança de atitude e uma nova visão, uma vez que deixou de “olhar” só para os factos passados para passar a “olhar” para o presente e futuro, tornando-se um apoio importante da gestão e, como tal, acresce valor à organização.

Com vista a este fim, acrescer valor, o Auditor Interno passa a ter um papel importante no processo de gestão de risco empresarial.

No âmbito da gestão de risco existem vários modelos dos quais salientamos o COSO a Norma AS/NZS 4360:29004, o COBIT, a norma sobre gestão de riscos – FERMA e a ISO 31000. De entre estes, o COSO e a Norma Australiana/Neozelandesa (AS/NZS 4360:2004), são modelos de referência de nível mundial na implementação de sistemas de gestão de risco empresarial e foram os principais pilares deste trabalho.

Através da aplicação prática, propusemo-nos demonstrar como é que se pode aplicar um modelo de gestão de risco nos trabalhos realizados pela Auditoria Interna, incluindo a matriz do risco inerente e matriz do risco residual, obtida depois de analisados os controlos, para além das recomendações propostas pela Auditoria Interna, tendo em vista a redução desse risco residual nos processos auditados.

Deste modo, com este trabalho pretendeu-se chamar a atenção para a importância da Gestão de Risco através da aplicação de um modelo de gestão de risco num processo de compras de uma organização. De salientar que não existe um modelo único, apenas existem referências que nos podem ajudar a adaptar a gestão de risco a determinada organização. Trata-se de um trabalho com alguma complexidade que exige conhecimentos adicionais, nomeadamente técnicas de gestão de risco e um conhecimento efectivo do negócio e das áreas a auditar.

Na aplicação prática foi efectuada uma análise do processo de compras de acordo com a metodologia de Gestão de Risco adoptada, incidindo apenas nas actividades desenvolvidas no Departamento de Compras. Desta forma, para que se possa apresentar uma visão transversal na Organização sobre o risco residual é necessário desenvolver

uma análise junto das restantes áreas operacionais onde os processos identificados ocorrem.

Assim sendo, depois de concluída a auditoria na Área de Compras, com a emissão das propostas de recomendação, a Auditoria Interna deverá facilitar o processo de avaliação do risco residual das compras nas restantes áreas operacionais não abrangidas na análise agora desenvolvida mas que estão já identificadas no capítulo de estabelecimento do contexto e que estão inter-relacionadas.

Esse trabalho permite, não só, introduzir o conceito de gestão de risco nessas áreas, com a apresentação da metodologia de gestão de risco e conclusões até ao momento apresentadas, como também, preparar o trabalho de campo nas áreas que a Auditoria Interna virá a realizar em momento posterior.

Como foi possível verificar ao longo da realização deste trabalho, esta abordagem da Auditoria Interna focada no risco do negócio proporciona um conhecimento exacto dos processos de negócio, sub-processos e actividades permitindo uma gestão mais eficaz dos riscos. Permite fixar o apetite ao risco e determinar o risco residual através da matriz de riscos, o que facilita a elaboração do plano de auditoria, uma vez que, a Auditoria Interna poderá concentrar-se nos riscos chave do negócio.

Embora haja em Portugal, no que respeita à Gestão de Risco Empresarial, um longo caminho a percorrer pelas nossas Empresas e Gestores, bem como, pelas nossas Escolas, entendemos que este trabalho poderá ser uma ajuda na implementação de um modelo de gestão de risco empresarial e deste modo fomentar a cultura de gestão de risco e sensibilizar para a sua importância no seio de uma organização.

BIBLIOGRAFIA

Almeida, Domingos; **2009**; *Auditoria Interna e Gestão do Risco*; XVI Conferência Anual do IPAI.

Almeida, Domingos; **2006**; *O Valor da Auditoria Interna*; Revista do IPAI nº 25; Outubro/Dezembro; págs. 3-4.

.

Azevedo, Belmiro; **2005**; *Gerir o Risco através da Criação de Valor*; Revista IPAI, nº 23; Janeiro/Março 2006.

Barros, Carlos; **2006**; *Dependência entre Risco e Inerente e Risco de Controlo*; Revista Revisores & Empresas; Abril/Junho; Pág.10 a 18.

Bastos, Alberto; **2009**; *Focaliza a ISO 31000* em Entrevista à Brasiliano&Associados (B&A); Revista de Gestão de Riscos nº 47; Setembro.

Beja, Rui; **2004a)**; *Risk Management – Gestão, Relato e Auditoria dos Riscos do Negócio*; Áreas Editora.

Beja, Rui; **2004b)**; *Relato e Auditoria dos Riscos do Negócio*; Comunicação efectuada no X Congresso de Contabilidade consultada em Novembro de 2009 em: http://www.ordemeconomistas.pt

Beja, Rui; **2004c)**; *Risk Management: Conceito, Âmbito e Procedimentos*; Artigo consultado em Novembro 2009 em: http://www.ordemeconomistas.pt

Blair, Colin; **2009**; *Gestão de Risco Eficaz*; Artigo consultado em http://www.standards.org.au/downloads/091120_New_Risk_Management_Standard.pdf

Câmara, Paulo; **2008**; *A Auditoria Interna e o Governo das Sociedades*; Revista do IPAI, nº 31; Julho/Setembro; págs.11-15.

Castanheira, Nuno; **2007**; *Auditoria Interna Baseada no risco: Estudo do caso Português*; Tese de Mestrado; Universidade do Minho; Junho.

Castanheira, Nuno; **Rodrigues**, Lúcia; **2006a)**; *Gestão de Risco – Da Abordagem Tradicional à Gestão de Risco Empresarial (ERM)*; Revista Revisores & Empresas; Julho/Setembro; pág. 58.

Castanheira, Nuno; **Rodrigues**, Lúcia; **2006b)**; *Mapa de Riscos - Ferramenta de Integração da Gestão de Riscos e da Auditoria Interna*; Revista do IPAI, nº 24; Julho/Setembro; pág.11.

Cicco, Francesco; **2010**; *Dos Rriscos "Negativos" aos Riscos "Positivos*" consultado em 20 Janeiro 2010 em http://www.iso31000qsp.org/

Cicco, Francesco; **2009**; *ISO 31000:2009 – Gestão de Riscos*; consultado em 20 Dezembro 2009 em; http://www.iso31000qsp.org/2009/08/29ago.html

Cicco, Francesco**; Fantazzini,** Mario**; 2003;** T*ecnologias consagradas de gestão de riscos*; Série Risk Management; Risk Tecnologia Editora Ltda; 2ª Edição Maio.

COBIT 4.1 Spanish; **2007**; *Resumen Ejecutivo*; IT Governance Institute; consultado em 09/10/2009 em: www.isaca.org.

Cocurullo, Antonio; **2008**; *Visão Estratégica e Gestão de risco*; Ernest&Young, consultado em Novembro 2009 em: http//www,prmia,org.

Cocurullo, Antonio; **2006**; Enterprise Wide Risk Management; Gerenciamento de Riscos Corporativos; Classificação de Riscos; Março.

Cocurullo, Antonio e **Vanca**, Paulo; **2002**; *A importância da Gestão de Riscos nos processos de Auditoria; PricewaterhouseCoopers*;

COSO – Committee of Sponsoring Organizations of the Treadway Commission; *Entreprise Risk Management* – Integrate Framework; **2004a)**; traduzido pelo Instituto de Auditores Internos de Espanha e PriceWaterHouseCoopers em 2009

COSO – Gerenciamento de Riscos Corporativos – Gestão Integrada – Sumário Executivo; **2004b);** tradução conjunta de AUDIBRA e PricewaterhouseCoopers

COSO – Committee of Sponsoring Organizations of the Treadway Commission; *Internal Control Integrate Framework*; **1992**; traduzido pelo Instituto de Auditores Internos de Espanha e Coopers&Lybrand, S.A. em1997.Ediciones Diaz de Santos, S.A.

Costa, Carlos; **2007**; Auditoria Financeira – teoria e prática; Editora Rei dos Livros; 7ª Edição.

Ferma; **2003**; Federation of European Risk Management Associations; *Norma de Gestão de Riscos.*

Ferreira, Luiz; **2002**; *Entendendo o COSO - Um Roteiro Prático para Entender os Princípios do COSO*; consultado em 27/07/2007: www.auditoriainterna.com.br/coso.htm.

Gonçalves, António; **2008**; *A Evolução das Metodologias de Auditoria*; Revista Revisores & Empresas; Julho/Setembro.

Hussein, Haji; **2008**; E- Commerce e Ressource Centre; Article; *Risk Assessement; Using COBIT® as a Guide Risk Assessement Assurande Services*, consultado em 06/'06/2009: http://fata86.webs.com/riskassesment.html.

IBCG - Instituto Brasileiro de Governança Corporativa; **2007**; *Guia de Orientação para Gerenciamento de Riscos Corporativos*.

IIA, *Normas Internacionais para o Exercício Profissional de Auditoria Interna*; **2009**; Tradução do IPAI.

IIA and Institute of Internal Auditors UK&Ireland ; **2004**; Declaración de Posición ; *El Rol de la Auditoria Interna en la Gestión de Riesgo Empresarial*. Consultado em: http://coso.org/chapters/pubdocs/264/Rol_del_Auditor_Interno_en_el_ERM[1].pdf

IIA, *Normas Internacionais para o Exercício Profissional de Auditoria Interna*; **1999**; Definição de Auditoria Interna; Tradução do IPAI.

IPAI (Instituto Português de Auditores Internos); 2002; *A Lei de Sarbanes-Oxley de **2002***; Resumo das principais cláusulas de interesse para os Auditores Internos**.**

IRAM, Instituto Argentino de Normalizacíon y Certifivación**; 2004;** *Normaria - Boletín de la Comissión de Normas e Asuntos Profesionales del Instituto de Auditores Internos de Argentina; Gestión de Riesgos*; Norma IRAM 17550 – Esquema A1; nº 18; Dezembro, consultado em 04/06/2009: http://www.iaia.org.ar/Normaria/Normaria18.pdf.

ISO – International Organization for Standardization; **2009**; *Novo padrão ISO para a gestão eficaz dos riscos*; http://www.modulo.com.br/site?infoid=800&lng=br&sid=91

Júnior, Odete; **2009**; Por uma gestão de risco eficiente; Artigo disponível na B2B Magazine; Outubro, consultado em 22 de Novembro 2009: http://www.b2bmagazine.com.br/web/interna.asp?id_canais=4&id_subcanais=17&id_noticia=24444

Junior, Sebastião**; 2005**; *Controles Internos como um Instrumento de Governança Corporativa*; Revista BNDES; Dezembro; Rio de Janeiro; Consultado em 29 Dezembro de 2009 em : http://www.bndes.gov.br/SiteBNDES/export/sites/default/bndes_pt/Galerias/Arquivos/conhecimento/revista/rev2406.pdf

KPMG – Auditores Consultores, Ltda; **2006**; *Entendiendo la Administración del Riesgo Empresarial - Um Modelo Emergente para Generar Valor al Accionista*; consultado a 08 Dezembro de 2009 em: http://www.kpmg.cl/aci/pdf/ERM.pdf.

Knight, Kevin; **2009**; *ISO – International Organization for Standardization*; *Novo padrão ISO para a gestão eficaz dos riscos*; http://www.standards.org.au/downloads/091120_New_Risk_Management_Standard.pdf

Lorenzo, Mariano; **2001**; *La Audítoría Interna orientada a los Processos*; Revista Partida Doble nº 124 (Julio /Agosto:78-85).

Martin, Javier; **Morales**, Federico; **2001**; *La Audítoría de ríesgos: Un caso práctíco*; Revista Partida Doble nº 124 (Julio /Agosto:86-91).

McNamee, David; **2000**; *Tarteting Business Risk*; The Internal Auditors (Oct. 46-51).

McNamee, David; **1997a**; *Auditoria Baseada em Riscos*: mudando o paradigma das auditorias internas, adaptado e actualizado por Cicco, Francesco; 2006**;** consultado em 25 de Setembro de 2009 em: http://www.qsp.org.br/auditoria_risco.shtml

McNamee, David; **1997b**; *A Auditoria Baseada no Risco*; tradução de Rocha, J.D.Almeida; Cadernos de Auditoria Interna – Ano 2, Nº1, Maio, 1999; Banco de Portugal.

Morais, Acácio; **2000**; *Sistemas de Controlo Interno. Gestão e Finalidades*; Cadernos de Auditoria Interna; Ano 3, Nº1 (Outubro); Banco de Portugal.

Morais, Georgina; **2008**; *A Importância da Auditoria Interna para a Gestão: O Caso das Empresas Portuguesas;* trabalho apresentado no 18º Congresso Brasileiro de Contabilidade, consultado em 26 de Novembro de 2009 em: http://www.ccontabeis.com.br/_htm/cbc18.htm

Morais, Georgina; **Martins**, Isabel; **2007**; *Auditoria Interna – Função e Processo*; Áreas Editora; 3ª edição.

Moro, A.E.F.**; 1999,** *El Mapa de Ríesgos de Negócio: bases para su elaboración*; Partida Doble, Octubre: 72-85.

Pereira, Eduardo ; **Bracalente**, Fernando; **Dinofre**, Marcelo; **Bernardinelli**, Mario; **2008**; *COSO – The Committee of Sponsoring Organizations of the Treadway Commission, consultado* em http:// infosegura.eti.br em 22 de Novembro de 2009.

Pinheiro*,* Joaquim Leite; **2008**; *Auditoria Interna – Auditoria Operacional - Manual Prático para Auditores Internos*; Editora Rei dos Livros.

PricewaterhouseCoopers; **2002**; *Business Risk Model*; http://globalbestpractices.pwc.com

Protiviti, Independent Risk Consulting; *Guide to Enterprise Risk Management*; **2006**; – www.protiviti.com.

QSP – *Centro da Qualidade, Segurança e Produtividade; **2010**; ISO 31000 Gestão de Riscos*; 28 Janeiro; Consultado em: http://www.iso31000qsp.org/

Sandonato, Franco; **2007**; *A Importância dos Frameworks de Controlo de Processos para a Gestão efectiva da Tecnologia da Informação*; XXVII Encontro Nacional de Engenharia de Produção; Brasil

Série Risk Management; **2007;** *Auditoria Baseada em Riscos – Como Implementar a ABR nas organizações: uma abordagem inovadora*; Revisão Técnica de Francesco De Cicco. Risk Tecnologia Editora Ltda.

Série Risk Management; 2005; *Directrizes para a Implementação da AS/NZS 4360:2004;* Revisão Técnica Francesco De Cicco¸ Agosto; Risk Tecnologia Editora Ltda.

Série Risk Management; 2004; *Gestão de riscos*: *A norma AS/NZS 4360:2004*; Revisão Técnica Francesco De Cicco; Risk Tecnologia Editora Ltda; 2ª Edição; Dezembro

Silva, António; **2006**; *Contextualização da Gestão e Auditoria do Risco*; Revista do IPAI, nº25: 10 a 12.

Simões, Reinaldo; **2009;** *Gestão de Riscos segundo as Normas AS/NZS 4360:2004 e ISO 31000:2009*; QSP- Centro da Qualidade, Segurança e Produtividade - consultado em 22 Nov.2009: http://www.abrapp.org.br/ppub/portal/adm/editor/UploadArquivos/30congresso/tecnicas/tec9/reinaldo_simoes.pdf.

Sousa, Orlando; **2007**; *Auditoria Interna – Evolução para além da Sabarnes-Oxley*; Revista nº 26 do IPAI (Janeiro/Março).

Standards Australia; Standards New Zealand; AS/NZS 4360**:2004;** Risk Management;

Standards New Zealand; AS / NZS ISO 31000:2009; **2009** - *Nova Norma Internacional sobre Gestão de Riscos*; Edição 10 de 9 de Outubro; consultado em 22 de Nov.2009: http://www.standards.co.nz/touchstone/Issue+10/Business/AS+NZS+ISO+31000+2009+new+in

Sumners, Glenn; **1999**; *El Futuro de la Auditoria Interna*; Revista Partida Doble, nº 103, Setembro: 92.

Veja, Luis; **2003**; *La Gestión de Ríesgos en Empresas no Financieras*; Revista Partida Doble, nº 150, Deciembre.

Willsher, Richard; **2007**, *Um negócio arriscado*; Revista Exame World Business; Agosto/Setembro/Outubro: 42 a 47.

Zárate, Fernando; **2001**; *La Gestión de Ríesgos: un enfoque prático*; Revista Partida Doble, nº 124, Jul./Ago.

Manual de Riscos de Negócio

Fonte: Adaptado Business Risk Model

Global Best Practice – PricewaterhouseCoopers

(Anexo 1)

RISCOS DO MEIO ENVOLVENTE 4

1. Disponibilidade de Capital 4
2. Perda Castatrófica 4
3. Concorrência 4
4 Mercados Financeiros 4
5. Industria 4
6. Legal 4
7. Normativo 4
8. Sensibilidade 5
9. Relacções com Accionista 5
10 Político 5

RISCOS DO PROCESSO 6

RISCOS OPERACIONAIS 6
11. Interrupção do Negócio 6
12. Capacidade 6
13. Cumprimento normas e regulamentos 6
14. Satisfação dos Consumidores 6
15. Tempo do Processo 6
16. Eficiência 6
17. Ambiental 6
18. Saúde s Segurança 7
19. Obsolescência 7
20. Recursos Humanos 7
21. Expectativas de Performance 7
22. Desenvolvimento de Produto 7
23. Falha de Produto/Serviço 7
24. Fornecimento 7
25. Perda de Valor das Marcas 7
RISCO DE AUTORIDADE 7
26. Autorização 8
27. Facilidade de Mudança 8
28. Comunicação 8
29. Liderança 8
30. Subcontratação 8
31. Incentivos performance 8
RISCO TÉCNOLÓGICO / PROCESSAMENTO DA INFORMAÇÃO 9
32. Acessos 9
33. Disponibilidade 9
34. Integridade 9
35. Infraestruturas 9
36. Relevância da Informação 9
RISCO DE INTEGRIDADE 10
37. Fraude do Colaborador 10
38. Actos Ilegais 10
39. Fraude da Gestão 10
40. Reputação 10
41. Uso Não autorizado 10

RISCO FINANCEIRO 11
42. Crédito – Colateral 11
43. Crédito - Concentração 11
44. Crédito - Escassez 11
45. Liquididez - Cash-Flow 11
46. Liquididez -Concentração 11
47. Preço - Câmbio 11
48. Preço - Capitais Próprios 11
49. Preço - Instrimentos Financeiros 11
50. Preço - Taxa de Juro 11

RISCOS DA INFORMAÇÃO PARA A TOMADA DE DECISÃO 12

RISCO OPERACIONAL 12
51. Alinhamento 12
52. Contratos/Compromissos 106
53. Avaliação Performance 12
54. Preço 12
55. Reporte Normativo (Operacional) 12
RISCO FINANCEIRO 12
56. Informação Contabilística 12
57. Orçamento 13
58. Avaliação da Informação de Gestão 13
59. Avaliação de Investimentos 13
60. Fundo de Pensões 13
61. Reporte Normativo (Financeiro) 13
62. Impostos 13
RISCO ESTRATÉGICO 14
63. Portefólio do Negócio 14
64. Avaliação do Ambiente do Negócio 14
65. Ciclo de Vida 14
66. Organização da Empresa 14
67. Avaliação Performance (Estratégica) 14
68. Planeamento 14
69. Alocação de Recursos 14
70. Valorização 14

RISCOS DO MEIO ENVOLVENTE

1. Disponibilidade Capital – Trata-se do risco de a organização não dispor de eficientes meios de acesso ao capital que necessita para o seu crescimento, para execução das suas estratégias e gerar retorno financeiro.

2. Perda Catastrófica - Risco de incapacidade em manter a operacionalidade ou de recuperar custos operacionais como resultado de uma catástrofe.

3. Concorrência - Risco de os principais concorrentes ou novos concorrentes actuarem de forma a obter vantagem competitiva (ex: qualidade superior, menor custo, etc.) sobre a Empresa podendo afectar a sua sobrevivência.
Estas acções incluem o desenvolvimento de novas propriedades do produto/serviço, Marketing e Vendas agressivo e efectivo, melhoria da qualidade, aumento da produtividade e redução de custos.

4. Mercados Financeiros- Risco de mudanças na capacidade de retorno ou no valor económico da Empresa como resultado de variações no mercado financeiro (ex: taxa de juro) que afectam os proveitos, custos ou rubricas de balanço.

5. Industria - Risco de a indústria perder a atractividade devido a mudanças, nos factores chave de sucesso competitivo dentro da indústria, incluindo oportunidades e ameaças significativas, na capacidade de manutenção no mercado e dos potenciais concorrentes, nos pontos fortes e fracos da Empresa em relação aos actuais e futuros concorrentes

6. Legal - Risco de as transacções, acordos estabelecidos contratualmente, estratégias específicas e actividades desenvolvidas pela Empresa não estarem conforme o estipulado na lei em vigor.

7. Normativo - Risco de alterações nas regulamentação e acções de entidades regulamentadoras, nacionais ou locais, que pode resultar no aumento de pressões competitivas e afectar significativamente a capacidade de a Empresa conduzir o negócio de forma eficiente.

8. Sensibilidade - Este risco resulta do comprometimento que a gestão faz dos recursos e cash flow esperados da Empresa até uma extensão tal que reduz a capacidade da Empresa para acompanhar as mudanças no ambiente em que se insere, que estão para além do seu controlo.

9. Relações com accionistas - Risco de falta de confiança por parte dos investidores (actuais e potenciais) por não entenderem as mensagens e estratégias da Empresa. Como resultado os investidores não terão a confiança necessária no potencial da Empresa para a obtenção do retorno do seu investimento.

10 Político - Risco de alterações políticas num país porem em causa os activos da Empresa ou a sua performance.

RISCOS DO PROCESSO

Risco Operacional

11. Interrupção do Negócio - O risco de incapacidade de manter em funcionamento operações ou processos críticos devido à elevada dependência de matérias-primas, tecnologias de informação, mão-de-obra especializada, etc.
Uma interrupção derivada da perda de Sistemas de Informação críticos, está descrita em mais pormenor na secção Risco de Processamento da Informação /Tecnologia - Disponibilidade.

12. Capacidade - Risco de a capacidade produtiva dos recursos humanos, não ser utilizada eficientemente e não ser adequada às necessidades e procura dos clientes

13. Cumprimento normas e regulamentos - Risco de falha no cumprimento de leis e regulamentos internacionais, nacionais e locais que se apliquem ao processo do negócio.

14. Satisfação dos consumidores- Risco de os processos de negócio não atingirem ou excederem, as expectativas dos clientes.

15. Tempo do processo - Risco de o tempo despendido desde o início até ao termo de um processo de negócio ser demasiado longo devido a passos irrelevantes, desnecessários e redundantes podendo resultar em perda de competitividade e oportunidade face aos concorrentes.

16. Eficiência - Riscos de os processos serem ineficientes na satisfação de pedidos válidos dos clientes, resultando em custos acrescidos face à concorrência.

17. Ambiental - Os riscos ambientais expõem a Empresa a potenciais responsabilidades avultadas, nomeadamente responsabilidades para com terceiros por prejuízos humanos ou materiais causados pela poluição e responsabilidades para com os governos ou terceiros por custos com a remoção de poluentes e por penalizações severas.

18. Saúde e Segurança - O risco de um inadequado controlo com a segurança e saúde dos trabalhadores resultar em responsabilidades com compensações a trabalhadores e causar uma reputação negativa.

19. Obsolescência - Risco de o produto da Empresa estar obsoleto/ultrapassado resultando em significativas perdas para a Empresa.

20. Recursos Humanos - Risco de os recursos humanos responsáveis pela gestão e controlo da organização ou do processo de um negócio não possuírem o conhecimento, capacidade e experiência necessária que assegure que os objectivos críticos são atingidos e que os riscos de negócio sejam reduzidos a um nível aceitável.

21. Expextativas Performance - Risco de a performance da Empresa ser desfavorável face à dos concorrentes devido a qualidade inferior, maiores custos e ou ciclos de tempo mais demorados.

22. Desenvolvimento do produto- Risco de o processo de desenvolvimento resultar num produto que o consumidor não quer ou não necessita, tem um custo que os consumidores não estão dispostos a pagar e por outro lado corresponde a uma necessidade mas é colocado no mercado tarde demais

23. Falha do Produto/Fornecimento - O risco de as operações existentes resultar em produtos defeituosos ou com desempenhos insuficientes.

24. Fornecimento - Risco de rupturas ou custos elevados devido a insuficiências no fornecimento de meios de produção, matérias-primas e outros recursos chave para as operações da Empresa. Este risco pode levar à incapacidade da Empresa satisfazer as necessidades dos clientes a preços competitivos, nas datas necessárias com a qualidade esperada.

25. Perda de Valor das Marcas - Risco de uma marca perder o seu valor durante o período de lançamento e de vida de um negócio.

Risco de Autoridade

26. Autorizações - O risco de as acções serem executadas por quem não tem autoridade e de descurar as acções que lhe são atribuídas.

Este risco ocorre quando colaboradores da empresa excedem as fronteiras de delegação ou autoridade, ocasionando situações de actos não autorizados, ilegais, não éticos ou assumem riscos de negócio não autorizados e inaceitáveis.

27. Facilidade de mudança - Risco de as pessoas na organização não estarem preparadas para implementar processos de melhoria suficientemente rápidos para fazer face às mudanças de mercado.

28. Comunicação - Risco de as comunicações, verticais e horizontais, dentro da organização serem ineficazes e resultarem em mensagens inconsistentes com as responsabilidades autorizadas ou medidas estabelecidas.

29. Liderança - Risco de as pessoas responsáveis pelos processos importantes do negócio não serem eficazes na execução de acções correctas.

30. Subcontratação - Existem dois tipos de risco com subcontratação:

⇒ Risco de fornecedores externos de serviços não agirem dentro dos seus limites de autoridade definidos e não actuarem de forma consistente com os valores, estratégias e objectivos da Empresa.

⇒ Risco de os processos estratégicos de negócio em regime de subcontratação poderem no final tornar a organização de subcontratação num concorrente da Empresa.

31. Incentivos Performance - Risco de gestores e empregados não "acreditarem" nas medidas de performance da Empresa por não serem realistas, compreensíveis, objectivamente determináveis ou executáveis de acordo com a estratégia e políticas da Empresa.

Risco Técnológico / Processamento de Informação

32. Accessos – Risco que o acesso à informação (dados ou programas) seja inadequadamente concedido ou recusado, o que significa a concessão de acessos a informação confidencial a pessoas não autorizadas ou incorrectamente autorizadas.

33. Disponibilidade - O risco da informação não estar disponível quando necessária. Os riscos incluídos incluem perda de comunicações (ex. corte de cabos, perda de centrais telefónicas), perda da capacidade básica de processamento (ex. causada por fogo, inundação, perda de energia) e dificuldades operacionais (ex. perda de discos, erros de operação). A indisponibilidade pode também ser causada por causas naturais, vandalismo, sabotagem e acidentes.

34. Integridade dos Sistemas de Informação - Este risco inclui todos os riscos associados com a autorização, totalidade e exactidão das transacções na sua introdução, processamento, sumarização e reporte nos diferentes sistemas aplicacionais da empresa.
Este risco aplica-se a todo e qualquer sistema da empresa, e a todos os aspectos de um sistema aplicacional, encontrando-se presente em diferentes locais e momentos.
A integridade pode ser perdida por erros de programas (ex. dados correctos processados por programas incorrectos), erros de processamento (ex. transacções são incorrectamente processadas mais do que uma vez sobre os mesmos ficheiros) ou erros de gestão (ex. gestão deficiente do processo de manutenção de sistemas).

35. Infraestruturas - risco de que a empresa não possua uma infra-estrutura tecnológica (ex. hardware, rede, software, pessoas e processos) que suporte de forma efectiva as necessidades actuais e futuras do negócio, de forma economicamente justificável e adequadamente controlada.

Estes riscos estão relacionados com os processos na área da tecnologia utilizados para definir, desenvolver, manter e operar o ambiente de processamento (ex. hardware e redes) e os sistemas aplicacionais associados (ex. suporte a clientes, facturação, stocks).

36. Relevância da Informação - Risco de a informação não ser relevante para atingir os objectivos para que foi recolhida, mantida ou distribuída.

Risco de Integridade

37. Fraude do colaborador - O risco de empregados, clientes ou fornecedores individualmente ou em conluio praticarem fraudes contra a empresa, resultando em perdas financeiras ou uso não autorizado de activos físicos, financeiros ou de informação.

Este risco pode levar a exposição legal, publicidade negativa ou adversa e impacto nas operações (perda de confiança dos clientes, fornecedores ou financiadores).

38. Actos Ilegais - Risco de colaboradores da empresa, individualmente ou em conluio, cometerem actos ilegais, colocando a empresa e os seus gestores em risco como consequência daqueles actos (ex. prisão, multas, sanções, suspensão de actividade, perda de receita, perda de clientes e perda de reputação).

39. Fraude da Gestão - Risco de a gestão emitir informação com intenção de enganar investigações públicas, auditores externos, ou envolver subornos, pagamento de influências e outros esquemas para benefício da Empresa.

40 Reputação - Risco de a Empresa perder clientes, empregados chave ou a sua capacidade para competir devido à percepção de que ela não age convenientemente com clientes, fornecedores e accionistas ou não sabe gerir o negócio.

41. Uso não autorizado - Risco dos activos físicos e financeiros serem utilizados para fins não autorizados ou não éticos por colaboradores ou outros e a informação e outros activos (Ex. desenhos de produtos, processos internos, listas de clientes, "know-how", e outros segredos) serem comprometidos por espionagem industrial, resultando numa perda de vantagens competitivas.

Risco Financeiro

42. Crédito - Colateral - Risco de o valor de um activo cedido como colateral para um empréstimo, recebimento ou obrigação poder perder parcial ou totalmente o seu valor.

43. Crédito - Concentração - Risco de perda excessiva como resultado de inapropriado ênfase do volume de vendas ou de receitas num único projecto, área geográfica, níveis de preço ou outro segmento económico.

44. Crédito - Escassez - O risco de crédito descreve a exposição a perdas reais ou custo de oportunidade, resultantes do incumprimento (ou outro tipo de falha) por uma entidade legal ou económica (o devedor) com o qual a Empresa possui relações de negócio.

Para empresas não financeiras, a gestão do risco de crédito é tipicamente induzida pela definição de requisitos de controlo sobre a base de clientes. O risco está relacionado com a entrega de bens ou prestação de serviços antes do recebimento do pagamento dos mesmos.

45. Liquidiez – Cash-Flow - Risco de perdas incorridas como resultado de incapacidade de financiamento das obrigações operacionais ou financeiras do negócio.

46. Liquidez - Concentração - Risco de perdas devido a incapacidade para liquidação de obrigações financeiras por concentração num reduzido número de fontes de financiamento que pode levar a dificuldade na obtenção de fundos quando necessários ou a um preço demasiado elevado.

47. Preço Câmbio - Risco de exposição a flutuações cambiais.

48. Preço - Capitais Próprios - Risco de flutuação do valor de participações em organizações detidas pela Empresa.

49. Preço – Instrumentos financeiros - Este risco varia em função do segmento de mercado em que o detentor do instrumento de financiamento está exposto, ou da forma como a exposição está estruturada.

50. Preço-Taxa de Juro - Risco associado à variação da taxa da juro.

RISCO DA INFORMAÇÃO PARA A TOMADA DE DECISÃO

Risco Operacional

51. Alinhamento - Risco de os objectivos e medidas de actuação dos processos de negócio não estarem alinhados com os objectivos e estratégias gerais da Empresa.

52. Contratos/Compromissos - Risco de a Empresa não ter acesso de forma eficiente e efectiva a informação sobre as responsabilidades contratuais vigentes em qualquer momento no tempo, por forma a que as decisões de comprometimento em responsabilidades acrescidas possam ser consideradas apropriadamente pelos decisores.

53. Avaliaçação da Performance (operacional) - Risco de a informação não constituir um retrato fiel da performance do negócio e não reflectir correctamente a realidade, não podendo assim servir de base para a decisão.

54. Preço - Risco na informação utilizada para a definição do preço. Este risco pode revelar-se de várias formas, isto é, o preço ser superior ao que os consumidores estão dispostos a pagar porque a política de preços da Empresa não se baseou em pesquisa de mercado nem na obtenção de outras informações sobre o consumidor ou então o preço não cobre os custos de desenvolvimento e produção.

55. Reporte normativo operacional - O risco que relatórios e informação operacional requerida pelas entidades reguladoras sejam incompletos, inexactos, fora de prazo, expondo a empresa a multas, penalidades ou sanções.

Risco Financeiro

56. Informação Contabilística - Risco de a informação financeira não ser suficiente e/ou ser manipulada, não servindo assim para a tomada de decisões.

57. Orçamento - Risco de o orçamento e planos não serem realista, não serem baseados em pressupostos correctos, não baseados nas performances do negócio, não aceites pelos Key managers, não úteis ou utilizados como ferramenta de monitorização.

58. Avaliação da Informação de Gestão - O risco que as demonstrações financeiras emitidas e utilizadas por investidores actuais ou futuros incluam erros materialmente relevantes ou omitem factos materialmente relevantes, tornando-as enganadoras.

Este risco resulta usualmente da incapacidade de obter informação de negócio relevante (de fontes internas ou externas) e de avaliar os ajustamentos necessários para representar fielmente a situação financeira da Empresa.

59. Avaliação de Investimentos - Risco de a gestão não ter informação financeira suficiente para tomar decisões sobre investimentos, ligando os riscos assumidos ao capital em risco.

60. Fundo de Pensões - Este risco inclui riscos associados à reputação, moralidade, litígios e necessidades de fundos adicionais.

61. Reporte Normativo (Financeiro) - Risco de os relatórios com informação financeira solicitados por agentes reguladores serem incompletos, imprecisos, inoportunos, sujeitando a Empresa a multas, penalidades e sanções.

62 Impostos - Este risco possui duas componentes chave que são o cumprimento de todas as leis/normas fiscais e transacções de valor materialmente relevante possuem impactos fiscais negativos que poderiam ser evitados se tivessem sido estruturadas de forma diferente.

Risco Estratégico

63. Portefólio do Negócio - Risco de a Empresa não possuir informação que lhe permita fazer uma gestão do seu "mix" de negócios de forma adequada.

64. Avaliação do Ambiente de Negócio - Este risco surge quando a Empresa não possui um processo efectivo de obtenção de informação relevante sobre o ambiente externo ou os pressupostos chave acerca do ambiente externo são inconsistentes com a realidade ou não são monitorizados pela Empresa.

65. Ciclo de Vida - Risco de uma Empresa não possuir informação para gestão do ciclo de vida de uma linha de produtos. Este risco tem impacto nas estratégias de negócio.

66. Organização da Empresa - Risco de a estrutura organizacional da Empresa não suportar uma mudança na estratégia de negócio da Empresa. Os valores e cultura de uma organização, as suas infraestruturas e a forma como estão definidas as responsabilidades, autoridades e margens e limites de actuação tem um impacto significativo na sua capacidade de gestão e alcance dos objectivos.

67. Avaliação da Performance (Estratégica) - Risco de as medidas de performance não serem suficientemente equilibradas, por exemplo: focam demasiado os resultados financeiros ou não serem consistentes, com as estratégias do negócio.

68. Planeamento - Risco de a estratégia de negócio da Empresa não ser dirigida por inputs criativos e intuitivos ou não ser baseada em pressupostos actuais sobre o ambiente externo da organização, resultando em estratégias desactualizadas e desfocadas.

69. Alocação de Recursos - Risco de o processo de afectação dos recursos da Empresa não estabelece nem sustenta uma vantagem competitiva nem maximizar o retorno para os accionistas.

70. Valorização - Risco de a gestão e os decisores não terem capacidade para medir de forma real o valor de um negócio ou um segmento específico no seu contexto estratégico.

ANEXO 2 - Matriz de Riscos Inerentes

Fase 2 do Modelo de GR - Identificar os Riscos

MATRIZ DE RISCOS (inerentes)PROCESSO: *1.1.2. Processo Geral - Compras Orçamento - Selecção do fornecedor e validação das condições*

RISCOS DO MEIO ENVOLVENTE

	A.I	
	I	P
1.Disponibilidade Capital		
2. Perda Castatrófica		
3. Concorrência		
4. Mercados Financeiros		

	A.I	
	I	P
5. Industria		
6. Legal	2	1
7. Normativo	1	1
8. Sensibilidade		

	A.I	
	I	P
9. Relações com accionistas		
10. Político		

RISCOS DO PROCESSO

RISCO OPERACIONAL	A.I I	A.I P
11. Interrupção do negócio	3	2
12. Capacidade		
13. Comprimento normas e regulamentos	3	2
14. Satisfação dos consumidores	2	2
15. Tempo do Processo	3	2
16. Eficiência	3	3
17. Ambiental		
18. Saúde e Segurança		
19. Recursos Humanos	3	2
20. Obsolescencia		
21. Expectativas de Performance		
22. Desenvolvimento de Produto		
23. Falha do Produto/Serviço	1	2
24. Fornecimento	3	3
25. Perda de Valor das Macas		

RISCO DE AUTORIDADE	A.I I	A.I P
26. Autoridade /Limite Risco	3	
27. Facilidade de Mudança		
28. Comunicação	3	2
29. Liderança	3	2
30. Subcontratação	3	2
31. Incentivos Performance		

PROCESSAMENTO INFORMAÇÃO / RISCO TECNOLÓGICO	A.I I	A.I P
32. Acessos	3	2
33. Disponibilidade	2	1
34. Integridade Sistemas de Informação		
35. Infrastructuras		
36. Relevancia da Iinformação		

RISCO DE INTEGRIDADE	A.I I	A.I P
37. Fraude do Colaborador	2	2
38. Actos Ilegais		
39. Fraude da Gestão		
40. Reputação	2	1
41. Utilização não autorizada	2	1

RISCO FINANCEIRO	A.I I	A.I P
42. Crédito - Colateral		
43. Crédito - Concentração		
44. Crédito- Escassez		
45. Liquididez - Cash Flow	1	1
46.Liquididez - Concentração		
47. Preço - Câmbio		
48. Preço Capitais Próprios		
49. Preço - Instrumentos Financeiros		
50. Preço - Taxa de Juro		

Legenda
I - Impacto (1 - Gerível; 2 - Importante 3 - Criítico)
P - Probabilidade (1 - Remota; 2 - Possível; 3 - Provável)

RISCOS DE INFORMAÇÃO PARA A TOMADA DE DECISÃO

RISCO OPERACIONAL	A.I I	A.I L
51. Alinhamento	2	1
52. Contratos/ Compromissos	3	2
53. Avaliação da Performance (Operacional)		
54. Preço		
55. Reporte normativo (Operacional)		

RISCO FINANCEIRO	A.I I	A.I L
56. Informação Contabilistica		
57. Orçamento	2	2
58. Avaliação Informação de gestão		
59. Avaliação de investimentos	1	2
60. Fundo de pensões		
61. Reporte normativo (Financeiro)		
62. Impostos		

RISCO ESTRATÉGICO	A.I I	A.I L
63. Portfólio do Negócio		
64. Avaliação do Ambiente do Negócio		
65. Ciclo de Vida		
66. Organização da Empresa		
67. Avaliação da Performance (Estratégica)		
68. Planeamento		
69. Alocaão de recursos		
70. Valorização		

Fonte: Adaptada da Business Risk Model - Global Best Practices -PricewaterhouseCoopers

ANEXO 2 - Matriz de Riscos Inerentes
Fase 2 do Modelo de GR - Identificar os Riscos

MATRIZ DE RISCOS (inerentes)PROCESSO: *1.1.4. Processo Geral - Compras Orçamento - Criação do Acordo de Fornecimento*

RISCOS DO MEIO ENVOLVENTE

	A.I	
	I	P
1.Disponibilidade Capital		
2. Perda Castatrófica		
3. Concorrência		
4. Mercados Financeiros		

	A.I	
	I	P
5. Industria		
6. Legal	1	1
7. Normativo	1	1
8. Sensibilidade		

	A.I	
	I	P
9. Relações com accionistas		
10. Político		

RISCOS DO PROCESSO

	A.I	
	I	P
RISCO OPERACIONAL		
11. Interrupção do negócio	3	2
12. Capacidade	1	1
13. Comprimento normas e regulamentos	1	1
14. Satisfação dos consumidores		
15. Tempo do Processo	3	2
16. Eficiência	2	2
17. Ambiental		
18. Saúde e Segurança		
20. Obsolescencia	1	2
19. Recursos Humanos		
21. Expectativas de Performance		
22. Desenvolvimento de Produto		
23. Falha do Produto/Serviço	3	2
24. Fornecimento	3	2
25. Perda de Valor das Macas		

	A.I	
	I	P
RISCO DE AUTORIDADE		
26. Autoridade /Limite Risco	3	2
27. Facilidade de Mudança		
28. Comunicação	2	2
29. Liderança	1	1
30. Subcontratação	3	2
31. Incentivos Performance		

	A.I	
	I	P
RISCO FINANCEIRO		
42. Crédito - Colateral		
43. Crédito - Concentração		
44. Crédito- Escassez		
45. Liquididez - Cash Flow	1	1
46.Liquididez - Concentração		
47. Preço - Câmbio	1	1
48. Preço Capitais Próprios		
49. Preço - Instrumentos Financeiros		
50. Preço - Taxa de Juro		

PROCESSAMENTO INFORMAÇÃO / RISCO TECNOLÓGICO	A.I	
	I	P
32. Acessos	3	2
33. Disponibilidade	1	1
34. Integridade Sistemas de Informação		
35. Infrastructuras	1	1
36. Relevancia da linformação		

	A.I	
	I	P
RISCO DE INTEGRIDADE		
37. Fraude do Colaborador	3	1
38. Actos Ilegais		
39. Fraude da Gestão		
40. Reputação		
41. Utilização não autorizada		

Legenda
I - Impacto (1 - Gerível; 2 - Importante 3 - Criítico)
P - Probabilidade (1 - Remota; 2 - Possível; 3 - Provável)

INFORMAÇÃO PARA A TOMADA DE DECISÃO

	A.I	
RISCO OPERACIONAL	I	P
51. Alinhamento	3	3
52. Contratos/ Compromissos	2	2
53. Avaliação da Performance (Operacional)		
54. Preço		
55. Reporte normativo (Operacional)	3	1

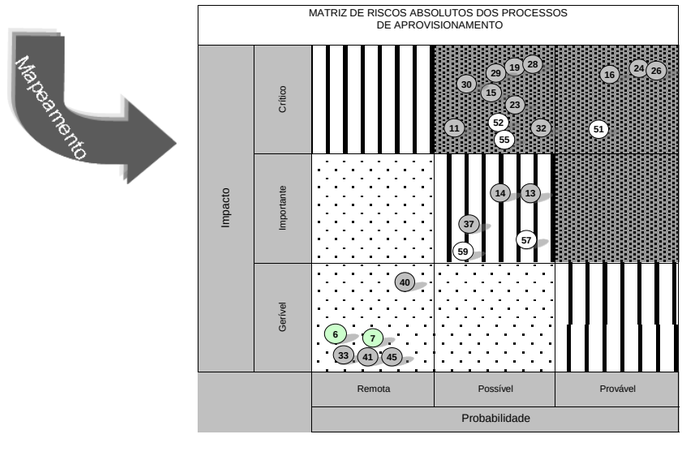
	A.I	
RISCO FINANCEIRO	I	P
56. Informação Contabilistica		
57. Orçamento		
58. Avaliação Informação de gestão		
59. Avaliação de investimentos		
60. Fundo de pensões		
61. Reporte normativo (Financeiro)		
62. Impostos		

	A.I	
RISCO ESTRATÉGICO	I	P
63. Portfólio do Negócio		
64. Avaliação do Ambiente do Negócio		
65. Ciclo de Vida		
66. Organização da Empresa		
67. Avaliação da Performance (Estratégica)		
68. Planeamento		
69. Alocação de recursos		
70. Valorização		

Fonte: Adaptada da Business Risk Model - Global Best Practices -PricewaterhouseCoopers

ANEXO 3 - Matriz de Riscos Inerentes
Fase 3 do Modelo de GR - Analisar os Riscos

Processos / Riscos		6. Legal	7. Normativo	11. Interrupção do negócio	13. Cumprimento normas e regulamentos	14. Satisfação do Consumidor	15. Tempo do Processo	16. Eficiência	19. Recursos Humanos	23. Falha de Produto/Serviço	24. Fornecimento	26. Risco de Autoridade	28. Comunicação	29. Liderança	30. Subcontratação	32. Acessos	33. Disponibilidade	37. Fraude do colaborador	40. Reputação	41. Utilização não autorizada	45. Liquididez - Cash Flow	51. Alignhamento	52. Contrato/Compromisso	55. Reporte normativo (Operacional)	57. Orçamento	59. Avaliação de Investimentos	Soma dos riscos	% Risco do Processo	Nº Ocorrências Risco Abs. >3
1.1. Compras Orçamento	1.1.2. Selecção do fornecedor e validação das condições	2	1	5	5	4	5	5	5	5	5	5	5	5	5	5	2	4	2	2	3	5	5	5	4	4	112	58%	18
	1.1.4. Criação do Acordo de Fornecimento	1	1	5	1	5	5	5	2	5	5	5	4	1	5	5	1	3	5	5	1	5	4	5	5	5	80	42%	12
	Nº Ocorrências	2	2	2	2	1	2	2	2	2	2	2	2	2	2	2	2	2	1	1	2	2	2	1	1	1			
	Nº Ocorrências [Risco Abs. >3]	0	0	2	1	1	2	2	1	2	2	2	2	1	2	2	0	1	0	0	0	2	2	1	1	1			



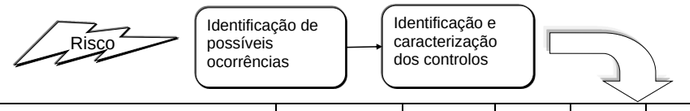
ANEXO 4 - Matriz de Análise de Riscos e Controlos

Fase 3 - Analisar os Riscos

Grupo de Compras - Materiais de Embalagem

Processo: 1.1. Processo Geral - Compras Orçamento

Fase 3 - Analisar o Risco



Sub-processos	Risco			Possível ocorrência	Descrição do Controlo		Controlos					
	Factor de Risco	Imp.	Prob.		Regulamentação Interna/Externa Aplicável	Outros Controlos	Objectivo do Controlo	Responsável pelo controlo	Classificação do Controlo I	II		IV
1.1.1. Elaboração dos orçamentos anuais de compras												
	11. Interrupção do Negócio Risco de interrupção do negócio	2	2	- Elevada dependência de um fornecedor, nomeadamente quando só exista um único fornecedor para determinado material crítico para a cadeia de abastecimento. Caso este fornecedor falhe, o negócio pode sofrer paragens se não for possível encontrar um fornecedor alternativo em tempo útil.	**Manual Procedimentos Controlo Interno:** Apenas devem ser consideradas na lista de fornecedores empresas que estejam em condições de fornecer o bem encomendado ou prestar o serviço requerido, que disponham de situação económica e financeira que garanta a continuidade do fornecimento. Fornecedores que forneçam materiais relevantes para a Qualidade, devem ser, sempre que possível, certificados por esta área antes de serem carregados nos dados-mestre.	- resposta do fornecedor ao inquérito enviado pelo Departamento de Compras e análise da mesma pela área de Qualidade	Minimizar o risco do fornecedor não ser capaz de cumprir os prazos de fornecimento e as quantidades necessárias ou os requisitos de qualidade do serviço/material estabelecidos	Gestores de Compras, Dir. Industrial, MKT e Qualidade	Primary	Operational	Manual	Preventive
				- Material comprado não cumpre com as características técnicas exigidas/necessárias. - Morosidade no processo de aprovação de um fornecedor pela área da qualidade	Sistema de Garantia da qualidade - normas internas/externas	Testes industriais, laboratoriais e conformidade efectuados aos materiais (amostras solicitadas ao fornecedor para o efeito)		Dir. Industrial e Qualidade	Primary	Operational / Compliance	Manual	Preventive
						Primeiros fornecimentos de pequenos montantes		Gestores Compras	Secondary	Operational	Manual	Preventive
						Recolha de informação através da Internet		Gestores Compras	Secondary	Operational	Manual	Preventive
						Comprometimento do fornecedor em fornecer os matérias de acordo com o estabelecido no caderno de encargos		Gestores Compras	Primary	Operational	Manual	Preventive
						- Visitas a feiras da especialidade em busca de novos fornecedores		Gestores Compras	Secondary	Operational	Manual	Preventive
				- Elevada dependência de um fornecedor - único fornecedor para determinado material	**Manual Procedimentos Controlo Interno:** Para os materiais estratégicos deverão existir fornecedores alternativos aprovados, de modo a reduzir-se o risco de eventuais rupturas de stock e garantir as melhores condições de fornecimento. No caso de fornecedor único deverão ser estabelecidas cláusulas contratuais que minimizem o risco de incumprimento de fornecimento e penalizações pelos danos resultantes do incumprimento dos prazos.			Dir. de Compras	Primary	Operational / Compliance	Manual	Preventive
	13. Cumprimento, Normas e Regulamentos Risco de incumprimento de regulamentos e normas externas e internas	2	2	- Incumprimento normas de Qualidade (**referidas no caderno de encargos**)	**Normas SGQ - Qualidade (internas/externas)**	É também efectuada uma Avaliação pela Qualidade aquando da recepção dos materiais em sistema informático.	Verificar se o fornecedor cumpre com o normativo legal exigido para o efeito	Dir. qualidade	Primary	operacional	System Based (SAP)	Detective
						Não é efectuado qualquer controlo na área de compras. Estas verificações são efectuadas pela área da Dir. Qualidade e podem traduzir-se em auditorias efectuadas às instalações do fornecedor.		Dir. qualidade	Primary	Operational/ Compliance	Manual	preventive / detective
						Comprometimento efectuado por escrito pelo fornecedor de que irá cumprir com o estabelecido no caderno de encargos.		Dir. Compras	Primary	Operational/ Compliance	Manual	Preventive
	14. Satisfação do Consumidor Risco da área de Compras não conseguir satisfazer as necessidades da área requisitante	2	2	Atraso na recepção dos orçamentos Várias versões de orçamento (por vezes com alterações significativas) morosidade no processo de aprovação de um novo fornecedor Área requisitante não está satisfeita com a qualidade do material ou com o modo como o Departamento de Compras desenvolveu o processo de aquisição do material Cliente não ficar satisfeito com a qualidade do produto (Ex.Materiais defeituosas que afectam a qualidade do produto)	**Manual Procedimentos Controlo Interno:** Para além da avaliação inicial que conduza à selecção de uma entidade como possível fornecedor, os fornecedores devem ser periodicamente avaliados quanto a: capacidade comercial; potencial técnico, nível de serviço quanto ao cumprimento das obrigações contratuais; nível de reclamações. Esta avaliação deve ser anual para os fornecedores de materiais relevantes para a Qualidade. Deverão ser efectuadas reclamações quando qualquer elemento especificado na encomenda ou contrato não foi cumprido por parte do fornecedor ou quando este entrega o material com defeito. As reclamações deverão ser efectuadas em documento próprio, devidamente fundamentadas e acompanhadas de todos os documentos necessários à reclamação. Fornecedores que forneçam materiais relevantes para a Qualidade, devem ser, sempre que possível, certificados por esta área antes de serem carregados nos dados-mestre.	O Departamento de Compras , no início de cada ano, retira as listagens de avaliação dos fornecedores (Sistema informático). Os fornecedores são avaliados em 3 parâmetros (**qualidade/quantidades/prazos**), o primeiro é da responsabilidade da Qualidade, o segundo e terceiro são da responsabilidade dos gestores de Stocks.	Verificar se as respectivas áreas cumprem os prazos de entrega da informação descritos no calendário de orçamento Avaliar a razoabilidade dos timings utilizados pela área da Qualidade para a aprovação e selecção de fornecedores. Ter em consideração a avaliação anual feita aos fornecedores pela área da Qualidade e Gestão de Stocks.	Respectivas áreas	Primary	Operational	Manual	preventive

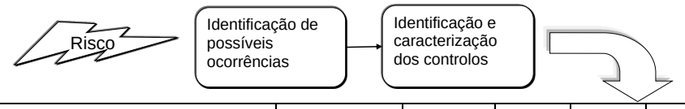
ANEXO 4 - Matriz de Análise de Riscos e Controlos

Fase 3 - Analisar os Riscos

Grupo de Compras - Materiais de Embalagem

Processo: 1.1. Processo Geral - Compras Orçamento

Fase 3 - Analisar o Risco



Sub-processos	Risco			Possível ocorrência	Descrição do Controlo		Controlos					
	Factor de Risco	Imp.	Prob.		Regulamentação Interna/Externa Aplicável	Outros Controlos	Objectivo do Controlo	Responsável pelo controlo	Classificação do Controlo I	II		IV
1.1.2. Selecção do fornecedor e validação das condições - 1.1.2.1. Actualização lista fornecedores - 1.1.2.2. Escolha do fornecedor a contactar - 1.1.2.3. Solicitação de cotação - 1.1.2.4. Análise comparativa propostas - 1.1.2.5. Selecção da proposta	**15. Tempo do Processo** Risco de actividades irrelevantes e redundantes atrasarem os processos de negócio do Grupo As situações apontadas para a ocorrência deste risco, enquadram-se, na nossa perspectiva no risco de eficiência, pelo que consideramos que o risco Cycle Time terá impacto reduzido nestes processos.	1	2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	16. Eficiência Risco de ineficiência na satisfação das necessidades dos clientes	1	3	Este risco está relacionado em parte, com o risco de Satisfação do consumidor, ou seja, o atraso na negociação das compras poderá por em causa a recepção dos materiais e por conseguinte a satisfação das necessidades dos clientes. Por outro lado, também é de referir que a morosidade do processo de aprovação de fornecedores poderá por em causa o processo de negociação com o fornecedor. Actividades que não acrescentam valor ao processo e/ou que motivam atrasos no processo de selecção Não existe uma filosofia de melhoria contínua dos processos	SGQ - Aprovação de fornecedores / selecção de fornecedores - Cadernos de encargos (Normas internas externas)	N/A	Garantir que os gestores de compras, não efectuem as compras, aproveitando as melhores condições/oportunidades por falta de informação da Dir. Qualidade (aprovação de fornecedor)	Gestores de compra	Secondary	Operational	Manual	Preventive
	19. Recursos Humanos Os colaboradores não possuem a experiência ou a capacidade necessária para o desempenho da função que lhe foi atribuída	1	2	A falta de experiência ou capacidade necessária para o desempenho da função, poderá por em causa o poder negocial da empresa e a realização de compras pouco competitivas, não aproveitamento das melhores oportunidades, selecção de fornecedores que não satisfaçam os requisitos da empresa.	N/A	- Experiência dos compradores e gestores de compras. - Acções de formação. - Compradores contactam a área requisitante com o intuito de se inteirarem das especificidades dos materiais para o qual estão a desenvolver o processo de compra de forma a poderem desenvolver o processo de negociação com os potenciais fornecedores - Nível de cumprimento do Contrato de Gestão da área das Compras e resultados das avaliações globais de desempenho.	Garantir que os compradores/ gestores de compras possuem a qualificação necessária ao desempenho das suas funções	Director de Compras	N/A Primary Primary Secondary	N/A Operational Operational Operational	N/A Manual Manual Manual	N/A Preventive Preventive Detective
	23. Falha de Produto/Serviço Risco dos clientes receberem produtos defeituosos ou ocorrerem falhas nos serviços contratados	1	2	Relativamente a esta questão, o problema coloca-se essencialmente pela não detecção atempada de anomalias nos materiais recepcionados. Esta situação poderá ocorrer quando o Departamento de Qualidade verifica que a recepção de materiais está conforme o certificado de garantia enviado pelo fornecedor, dando o OK, e posteriormente se verifica que os materiais não estão de facto todos em conformidade, tendo dado origem a produtos acabados e colocados no mercado com defeito. Fornecedor seleccionado não é capaz de fornecer produto com as especificações acordadas com a Empresa	Cumprimentos dos cadernos de encargos (normas internas/externas)	Certificado de garantia enviado pelo fornecedor juntamente com os matérias. Avaliação anual de fornecedores	Garantir que todos os materiais utilizados no processo produtivo, satisfaçam todos os requisitos exigidos, evitando a produção e venda de produtos irregulares.	Gestores de compra Gestores de compra, Qualidade, Gestores de Stocks	primary Primary	Operational Operational	Manual Manual	Preventive Detective
	24. Fornecimento Risco de não existir no mercado o material/serviço com o preço/qualidade desejado pela Unidade de Negócio	1	3	Não existir no mercado o material desejado pela área requisitante no que respeita aos níveis de qualidade necessários ou se existe o fornecedor não tem capacidade para responder às necessidades da empresa. Elevada dependência da empresa quando exista apenas um fornecedor para o material desejado.	**Manual Procedimentos Controlo Interno:** No caso de fornecedor único deverão ser estabelecidas cláusulas contratuais que minimizem o risco de incumprimento de fornecimento e penalizações pelos danos resultantes do incumprimento dos prazos. **SGQ- Sistema de garantia da qualidade -** No caderno de encargos estão referidos os normativos legais e as especificidades a que o fornecedor se obriga a cumprir.	De acordo com o descrito no caderno de encargos : 3.4 Controlo a Efectuar pela Empresa 3.4.1 Na recepção • Inspecção visual ao lote aquando da descarga. • Controlo laboratorial conforme o Plano de Inspecção e Ensaio (P.I.E.) da Empresa. A amostragem deve ser aleatória e terá como suporte as regras de amostragem de controlo por atributos, nomeadamente a Norma aplicável.	Garantir que os matérias cumprem os requisitos exigidos e descritos no caderno de encargos Garantir que são tomadas todas as medidas para evitar elevada dependência num fornecedor	Dir. Qualidade Dir. Compras	Primary Primary	Operational / Compliance Operational	Manual Manual	preventive / detective Preventive
	26. Autorização Risco dos colaboradores executarem tarefas que não era suposto ou não executarem as tarefas que lhes estavam atribuídas	1	3	Realização de negociações e comprometimento com fornecedores para as quais não tem poderes para exercer. Processo de selecção não teve o envolvimento do Gestor Compra ou Director de Compras apesar dos valores negociados no acordo assim obrigarem, considerando os níveis de autorização definidos internamente. Risco de não estarem definidas as regras de aprovação necessárias para validação das condições negociadas/acordadas levando a que os colaboradores desconheçam até que níveis t/m autonomia para negociar e formalizar acordos com os fornecedores.	Manual de Controlo Interno É obrigatório submeter à aprovação do requisitante os pedidos de compra que não forem executados no prazo requerido ou que exceda 10% do valor estimado- Instrução operacional - níveis de delegação	Análise por parte do Director de Compras dos processos de compra para um período (geralmente é feito mensalmente), verificando entre outros o cumprimento dos níveis de autorização, nomeadamente para os pedidos de montantes mais significativos	Assegurar que toda a actividade de compra é válida e está devidamente autorizada	Dir. Compras Director de Compras	Primary Primary	Compliance Compliance	Manual Manual	Corrective Detective

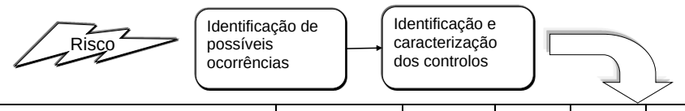
ANEXO 4 - Matriz de Análise de Riscos e Controlos

Fase 3 - Analisar os Riscos

Grupo de Compras - Materiais de Embalagem

Processo: 1.1. Processo Geral - Compras Orçamento

Fase 3 - Analisar o Risco



Sub-processos	Risco			Possível ocorrência	Descrição do Controlo		Controlos					
	Factor de Risco	Imp.	Prob.		Regulamentação Interna/Externa Aplicável	Outros Controlos	Objectivo do Controlo	Responsável pelo controlo	Classificação do Controlo I	II		IV
	28. Comunicação Risco da comunicação horizontal e vertical não ser eficiente resultando em mensagens inconsistentes com os objectivos propostos e a estratégia do grupo	1	2	Falha de comunicação vertical nos objectivos e políticas que devam ser considerados no processo negocial			Garantir uma comunicação eficaz entre os vários intervenientes no processo de compra	N/A	N/A	N/A	N/A	N/A
				Falha na comunicação entre compradores e fornecedores	**Manual de Procedimentos de Controlo Interno** A consulta ao fornecedor deverá ser efectuado mediante envio de caderno de encargos ou fichas técnicas dos bens ou serviços sempre que a denominação do bem não for o bastante para especificar o material ao fornecedor	Fornecedor deve sempre confirmar por escrito o resultado final das negociações, se não o fizer o comprador envia para o fornecedor um resumo com o que ficou acordado na reunião.		Gestores de Compras, Compradores	Primary	Operational	Manual	Preventive
					Manual de Procedimentos de Controlo Interno Solicitações aos fornecedores deverão ser efectuadas por escrito.							
	29.Liderança Risco dos responsáveis pelos processos críticos da empresa e liderança de equipas não terem o perfil adequado ao desempenho das funções que lhe foram cometidas	1	2	Chefia não transmite às suas equipas as orientações recebidas por parte da Gestão			Garantir que os líderes de equipa coordenam e supervisionam eficazmente o trabalho dos seus subordinados	N/A	N/A	N/A	N/A	N/A
	30. Subcontratação Risco dos fornecedores de serviços em outsorcing não actuarem de acordo com os limites e competências que lhes foram atribuidos e não agirem de acordo com os valores, estratégia e objectivos da organização.	1	2	A selecção e a negociação do fornecimento de determinados materiais de mebalagem, é efectuado por uma empresa do grupo, para todo grupo. Risco de não existir qualquer nível de controlo e de intervenção da Empresa no processo.			Garantir que os materias cumprem os requisitos exigidos e descritos no caderno de encargos	Dir. Qualidade	N/A	N/A	N/A	N/A
	37. Fraude do Colaborador Risco de empregados, clientes ou fornecedores individualmente ou em conluio praticarem fraudes contra a empresa	1	2	Selecção do fornecedor por parte do comprador obedecer a outros critérios que não a relação qualidade/preço do produto retirando proveito próprio desse processo.	Respeito pela normas éticas		Salvaguarda dos interesses da Empresa	Dir. Compras Chefias	Primary	Operational	Manual	Preventive
					Código de Ética da Empresa, caso exista.			Dir. Compras	Primary	Operational / Compliance	Manual	Preventive/ Detective
					Instrução operacional da Dir. Compras - Delegação de competências			Dir. Compras	Primary	Operational / Compliance	Manual	Preventive/ Detective
	Riscos Considerados não aplicáveis ou de Impacto/Probabilidade de Ocorrência reduzida na sequência da análise desenvolvida pela Auditoria Interna											
	32. Acessos	1	2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	40. Reputação	1	2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	51. Alinhamento	1	2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	52. Contratos/Compromissos	1	2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	57. Orçamento	1	2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	59. Avaliação de Investimentos	1	2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
		1	2		**SGQ- Sistema de garantia da qualidade** - No caderno de encargos estão referidos os normativos legais e as especificidades a que o fornecedor se obriga a cumprir.	O **Técnico da qualidade** aquando da recepção dos materiais verifica se o certificado que acompanha os materiais está ou não em conformidade com o contratualizado com o fornecedor e referenciado no caderno de encargos do material.	Verificar que os materiais estão em conformidade com os normativos externos e com as exigências da empresa.	Dir. qualidade	Primary	Operacional	SAP	Detective

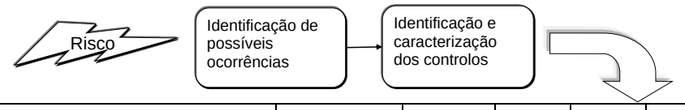
ANEXO 4 - Matriz de Análise de Riscos e Controlos

Fase 3 - Analisar os Riscos

Grupo de Compras - Materiais de Embalagem

Processo: 1.1. Processo Geral - Compras Orçamento

Fase 3 - Analisar o Risco



Sub-processos	Risco			Possível ocorrência	Descrição do Controlo		Controlos					
	Factor de Risco	Imp.	Prob.		Regulamentação Interna/Externa Aplicável	Outros Controlos	Objectivo do Controlo	Responsável pelo controlo	Classificação do Controlo I	II		IV
1.1.4. Criação do Acordo de Fornecimento	**13. Cumprimento, Normas e Regulamentos** Risco de incumprimento de regulamentos e normas externas e internas Risco considerado importante na sequência da análise realizada pela Auditoria Interna, apesar de ter sido classificado inicialmente pelo Gestor como pouco significativo.	1	1	O fornecedor comprometer-se com a empresa no cumprimento das normas referenciadas no caderno de encargos e na realidade não cumprir. Ocorrência de penalidades por incumprimento regulamentação legal aplicável aos materiais adquiridos	**Condições contratualizadas**	Gestor de compras valida a informação recebida do fornecedor, relativamente à base de cálculo das penalidades	Garantir o cumprimento das condições acordadas no contrato	Dir. Compras	Primary	Compliance	manual	Detective
	15. Cycle Time Risco de actividades irrelevantes e redundantes atrasarem os processos de negócio do Grupo As situações apontadas para a ocorrência deste risco, enquadram-se, na nossa perspectiva no risco de eficiência, pelo que consideramos que o risco Cycle Time terá impacto reduzido nestes processos.	1	2	Idem	Idem	Idem	Idem	Idem	Idem	Idem	Idem	Idem
	16. Efficiency Risco de ineficiência na satisfação das necessidades dos clientes	2	2	- Demora na criação do acordo de fornecimento causando atrasos nas divisões de remessa e no envio dos materiais para a área requisitante	N/A	Uma das medidas para aferir os níveis de serviço da performance dos compradores é a análise do tempo que medeia a liberação das requisições de compra e a criação do acordo de fornecimento. Semanalmente é retirada do SAP uma listagem das requisições liberadas a mais de 15 dias. Esta informação é analisada pelos Gestores de Compras e Director de Compras no sentido de se resolver as questões que se encontram pendentes e efectuar a criação do acordo de fornecimento.	Garantir a eficiência do processo de compras na satisfação das necessidades dos clientes	Gestor de Compra/ Director de Compra	Primary	Operational	System Based Controls	Detective
				- Atrasos na criação de acordos de fornecimento consequência da não criação e liberação das requisições	N/A	Compradores contactam a área requisitante pedindo a criação e liberação da requisição de modo a que possam criar o acordo de fornecimento.		Dir. Compras	Secondary	operational	Manual	Corrective

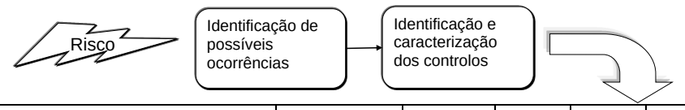
ANEXO 4 - Matriz de Análise de Riscos e Controlos

Fase 3 - Analisar os Riscos

Grupo de Compras - Materiais de Embalagem

Processo: 1.1. Processo Geral - Compras Orçamento

Fase 3 - Analisar o Risco



Sub-processos	Risco			Possível ocorrência	Descrição do Controlo		Controlos					
	Factor de Risco	Imp.	Prob.		Regulamentação Interna/Externa Aplicável	Outros Controlos	Objectivo do Controlo	Responsável pelo controlo	Classificação do Controlo			
									I	II		IV
	26. Authority/ Limit Risk Risco dos colaboradores executarem tarefas que não era suposto ou não executarem as tarefas que lhes estavam atribuídas Risco considerado importante na sequência da análise realizada pela Auditoria Interna, apesar de ter sido classificado inicialmente pelo Gestor como pouco significativo.	1	2	- Acordo de fornecimento não estar aprovado e assinado de acordo com os níveis de autorização definidos pela Área de Compras.	**Manual de Procedimentos de Controlo Interno** Secçãoxx - Níveis de Autorização	- O acordo de fornecimento deve estar assinado pelo Comprador e/ou Gestor de Compra e/ou Director de Compra de acordo com o documento interno que define os níveis de autorização.	Garantir que os colaboradores executam as tarefas que lhes estão cometidas	Gestor de Compra/ Director de Compras	Primary	Compliance	Manual	Preventive
	32. Access Risco do acesso à informação /sistemas de informação ser indevidamente concedido ou recusado.	1	2	- Criação ou alteração do acordo de fornecimento por pessoal não autorizado - Possibilidade de acesso a informação reservada por pessoas não autorizadas	N/A	Acessos a transacções do sistema de informação de criação e alteração concedidos somente a pessoal autorizado	Garantir que os acessos às transacções de criação e alteração de acordo de fornecimento estão devidamente controlados.	N/A	N/A	N/A	N/A	N/A
	37. Fraude do Colaborador Risco de empregados, clientes ou fornecedores individualmente ou em conluio praticarem fraudes contra a empresa **Considerado risco reduzido neste sub-processo**	1	1									
	Riscos Considerados não aplicáveis ou de Impacto/Probabilidade de Ocorrência reduzida na sequência da análise desenvolvida pela Auditoria Interna											
	11. Interrupção do Negócio	1	2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	15. Tempo do Processo	1	2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	23.Falha de Produto/serviço	1	2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	24. Fornecimento Risco de não existir no mercado o material/serviço com o preço/qualidade desejado pela Unidade de Negócio	1	2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	28. Comunicação	1	2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	30. Subcontratação	1	2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	51. Alinhamento	1	1	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	52. Contratos/ Compromissos	1	2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	55. Reporte normativo	1	2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

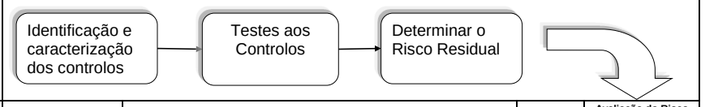
ANEXO 4 - Matriz de Análise de Riscos e Controlos

Fase 4 - Avaliar os Riscos

Grupo de Compras - Materiais de Embalagem

Processo: 1.1. Processo Geral - Compras Orçamento

Fase 4 - Avaliar os Riscos



Sub-processos	Risco						Avaliação do controlo	Avaliação do Risco após análise do controlo	
	Factor de Risco	Imp.	Prob.	Testado (Sim/Não)	Plano de Testes	Resultados dos testes efectuados	Nota	Imp.	Prob.
1.1.1. Elaboração dos orçamentos anuais de compras									
	11. Interrupção do Negócio Risco de interrupção do negócio	2	2	Sim	1 - Aferir por inquérito à área das Compras de situações de interrupção do negócio originadas por falha do fornecimento de um fornecedor.	1 -Não houve interrupção da produção motivada por atraso na aprovação de um fornecedor.	N/A	2	1
				Sim	2 - verificar a existência de resposta do fornecedor ao inquérito enviado pela área de compras	2 - Relativamente ao processo de aprovação do fornecedor de materiais de embalagem, existe resposta ao inquérito por parte dos fornecedores.	Bom		
				Sim	3 - Confirmar o tipo de testes que são efectuados (Testes industriais, laboratoriais e conformidade efectuados aos materiais (amostras solicitadas ao fornecedor para o efeito)	N/A controlo realizado fora da área das Compras	Não Avaliado		
				Sim	4 - Verificar se existe evidência da Recolha de informação de potenciais fornecedores através da Internet	4 - Não existe evidência desta recolha	insuficiente		
				Sim	5 - Verificar a existência do documento de Comprometimento do fornecedor em fornecer os matérias de acordo com o estabelecido no caderno de encargos	5 -Existe documento de comprometimento por parte do fornecedor. Este documento compromete o fornecedor a cumprir o estipulado no caderno de encargos.	Bom (se a recepção do doc.for atempada)		
				Sim	6 - Verificar se estarão definidas cláusulas com penalidades por incumprimento dos contratos celebrados com fornecedores	6 - Na maioria dos casos não estão definidas estas clausulas, porque não existe um contrato formalizado com o fornecedor.	Bom		
				Sim	7 - Verificar a % de compras atribuídas a um novo fornecedor.	7 - O critério utilizado na atribuição das quantidades a fornecer a cada fornecedor é o melhor preço, associado a este factor está o factor risco da dependência de um único fornecedor. A inclusão de fornecedores novos tem com objectivo trazer maior competitividade e um maior poder negocial.Contudo as quantidades inicialmente compradas são reduzidas.	Bom		
	13. Cumprimento, Normas e Regulamentos Risco de incumprimento de regulamentos e normas externas e internas	2	2	Não	N/A	N/A	Não Avaliado	2	
				Não	N/A	N/A	Não Avaliado		
				Não	N/A	N/A	Bom (se aplicado)		
	14. Satisfação do Consumidor Risco da área de Compras não conseguir satisfazer as necessidades da área requisitante	2	2	Sim	Questionário efectuado directamente aos gestores de compras	A resposta obtida foi de que por vezes, o orçamento não chega atempadamente, ou quando chega é posteriormente alterado, o que provoca atrasos no início do processo de compra. Esta situação pode originar perda de competitividade e oportunidade negocial. A área de compras elabora no final de cada ano e tendo como base a avaliação efectuada aos fornecedores pelas áreas de Qualidade e Gestão de stocks, informando-o da classificação obtida, bem como do critério utilizado na avaliação. Foi-nos facultada cópia duma carta enviada em Março de 2007, relativa à avaliação de 2006 - Ex. Fornecedor Alcoa Deutshchand GMBH. De referir que a avaliação dos fornecedores não é tida em consideração na selecção de um fornecedor, por considerarem que a mesma não é rigorosa, no que diz respeito à avaliação feita pelo gestor de stocks.	Insuficiente	2	

ANEXO 4 - Matriz de Análise de Riscos e Controlos

Fase 4 - Avaliar os Riscos

Grupo de Compras - Materiais de Embalagem

Processo: 1.1. Processo Geral - Compras Orçamento

Fase 4 - Avaliar os Riscos

Identificação e caracterização dos controlos → Testes aos Controlos → Determinar o Risco Residual

Sub-processos	Risco			Testado (Sim/Não)	Plano de Testes	Resultados dos testes efectuados	Avaliação do controlo	Avaliação do Risco após análise do controlo	
	Factor de Risco	Imp.	Prob.				Nota	Imp.	Prob.
1.1.2. Selecção do fornecedor e validação das condições - 1.1.2.1. Actualização lista fornecedores - 1.1.2.2. Escolha do fornecedor a contactar - 1.1.2.3. Solicitação de cotação - 1.1.2.4. Análise comparativa propostas - 1.1.2.5. Selecção da proposta	**15. Tempo do Processo** Risco de actividades irrelevantes e redundantes atrasarem os processos de negócio do Grupo As situações apontadas para a ocorrência deste risco, enquadram-se, na nossa perspectiva no risco de eficiência, pelo que consideramos que o risco Cycle Time terá impacto reduzido nestes processos.	3	2	N/A	N/A	N/A	N/A		
	16. Eficiência Risco de ineficiência na satisfação das necessidades dos clientes	3	3	Sim	Questionário efectuado aos gestores de compras	A informação não chega atempadamente, ou quando chega é posteriormente alterada, o que provoca atrasos no início do processo de compra. Esta situação pode originar perda de competitividade e oportunidade negocial. A situação descrita anteriormente também se aplica, quando um processo de aprovação de fornecedores é muito moroso. Verificamos que não existem tempos definidos por parte dos intervenientes, para a aprovação de fornecedores.	Insuficiente	2	
	19. Recursos Humanos Os colaboradores não possuem a experiência ou a capacidade necessária para o desempenho da função que lhe foi atribuída	3	2	Não	Qustionar sobre a qualificação e experiência dos seus colaboradores	Os gestores de compras possuem formação e experiência adequada para o desempenho sa sua função	Bom		
				Sim	Questionar os compradores sobre as suas necessidades de formação e a adequação da formação ministrada.	Tem frequentado acções de formação, são adequadas à função e a frequência é boa.	Bom (Necessário avaliação mais profunda para devida aferição do risco)		
				Não	N/A	N/A	Não Avaliado	2	
				Não	N/A	N/A	Não Avaliado		
	23. Falha de Produto/Serviço Risco dos clientes receberem produtos defeituosos ou ocorrerem falhas nos serviços contratados	3	2	Não	N/A	N/A	Bom (se aplicado)		
				Sim	1- Análise de um processo de compra: verificar se existe evidência de que os compradores/ gestores tiveram em consideração os resultados da avaliação dos fornecedores no processo de selecção do fornecedor.	1- De acordo com informação dos gestores de compras, no processo de selecção de fornecedores, não são tidas em consideração as avaliações anuais efectuadas a fornecedores pela área da qualidade e gestão de stocks.	insuficiente	2	
	24. Fornecimento Risco de não existir no mercado o material/serviço com o preço/qualidade desejado pela Unidade de Negócio	3	3	Não	Acordos de fornecimento demateriais de embalagem	A compra de determinados matetiais de embalgem é efectuada com base num contrato negociado por uma empresa do grupo, para todo o grupo e cuja intervenção da área de compras é meramente ao nível da formalização do acordo de fornecimento, tendo por base a informação recebida da empresa que contratualiza. Esta Empresa não tem qualquer intervenção no processo negocial.	N/A		
				Não	N/A	Controlo efectuado fora da área de compras	Não Avaliado		
				Não	N/A	N/A	Bom (se aplicado)		

ANEXO 4 - Matriz de Análise de Riscos e Controlos

Fase 4 - Avaliar os Riscos

Grupo de Compras - Materiais de Embalagem

Processo: 1.1. Processo Geral - Compras Orçamento

Fase 4 - Avaliar os Riscos

Identificação e caracterização dos controlos → Testes aos Controlos → Determinar o Risco Residual

Sub-processos	Risco						Avaliação do controlo	Avaliação do Risco após análise do controlo	
	Factor de Risco	Imp.	Prob.	Testado (Sim/Não)	Plano de Testes	Resultados dos testes efectuados	Nota	Imp.	Prob.
	26. Autorização Risco dos colaboradores executarem tarefas que não era suposto ou não executarem as tarefas que lhes estavam atribuídas	2	1	Não	3 - Inquérito ao Director de Compras questionando situações em que tenha constatado que os Compradores/ Gestor de Compra não o envolveram num processo de compra quando assim o deveriam de acordo com o documento interno de níveis de autorização.	3 - Não foram relatadas pelo Director de Compras situações em que tenha detectado o incumprimento dos níveis de autorização.	Bom	2	1
	28. Comunicação Risco da comunicação horizontal e vertical não ser eficiente resultando em mensagens inconsistentes com os objectivos propostos e a estratégia do grupo	2	2	N/A	N/A	N/A	N/A	2	2
				Sim	Inquérito aos compradores sobre a realização da acta da reunião, ou realização de uma informação com os principais pontos referidos na mesma e assinada pelo fornecedor	A resposta obtida foi de que por norma não são efectuadas actas das reuniões, nem existe por parte da área de compras um documento (modelo), onde se identificam as condições negociadas e se solicita ao fornecedor para assinar, ficando deste modo o fornecedor comprometido com as condições negociadas.	Insuficiente		
	29.Liderança Risco dos responsáveis pelos processos críticos da empresa e liderança de equipas não terem o perfil adequado ao desempenho das funções que lhe foram cometidas	2	2	N/A	Inquérito aos gestores de compras, procurando ouvir relatos de insatisfação face às medidas tomadas pela sua chefia directa (Director de Compras), situações em que se sintam pouco apoiados pela chefia, e tarefas para as quais consideram que lhes poderiam ser delegadas.	A sua chefia directa (director de compras) transmite toda a informação necessária para o bom desempenho da sua função. O Responsável pela área de compras está disponível para quaisquer esclarecimentos adicionais.	Bom (Necessário avaliação mais profunda para devida aferição do risco)	2	
	30. Subcontratação Risco dos fornecedores de serviços em outsorcing não actuarem de acordo com os limites e competências que lhes foram atribuidos e não agirem de acordo com os valores, estratégia e objectivos da organização.	2	2	N/A	Verificar como são efectuados os acordo de fornecimento dos materiais de embalagem e qual a intervenção no mesmo por parte da Empresa.	Verificamos que a compra de determinados materiais de embalagem são efectuados com base em contrato negociado por outra empresa do Grupo e cuja intervenção da área de compras é meramente ao nível da formalização do acordo de fornecimento. A Empresa não tem qualquer intervenção no processo de compras destes materias. Não são executados testes que nos permitam afirmar que estamos perante o melhor preço, isto porque, considera o Dir. de Compras que o poder negocial desta empresa do grupo é de tal ordem, que dificilmente se iriam conseguir melhores preços.	Não Avaliado	2	
	37. Fraude do Colaborador Risco de empregados, clientes ou fornecedores individualmente ou em conluio praticarem fraudes contra a empresa	2	2	Não	N/A	N/A	Não Avaliado	2	
				Sim	Questionar o Responsável do departamento de compras quanto à divulgação (fornecedores e colaboradores da área de compras) do código de ética do grupo e ao acompanhamento do seu cumprimento.	1 - A Área de Compras segue o código de ética e inclusivé enviou aos fornecedores que considerou como sendo os mais importantes para o grupo, uma carta onde apresenta as directivas para os fornecimentos à Empresa aqual anexou o Código de Ética do grupo. Não obtivémos evidência do envio destas cartas a fornecedores estrangeiros, nem aos novos fornecedores com os quais a Empresa prevê manter uma relação de continuidade.	Suficiente		
				Sim	Análise dos processos seleccionados para amostra e verificação da evidência de validação/aprovação das condições negociadas de acordo com as normas internas do departamento de Compras	O gestor de compras tem em consideração a listagem existente de fornecedores aprovados para cada grupo de material, pelo que, estes fornecedores são os escolhidos para solicitar propostas (cotações), no entanto, nada invalida de contactarem novos fornecedores (mesmo sem estarem a provados). São recolhidas as propostas pelos compradores e posteriormente é feita uma análise comparativa das mesmas e apresentadas ao Director de Compras para avaliar e decidir quanto à proposta a seleccionar. **De referir que não existe evidência desta aprovação por parte do Director de Compras.** Caso se venha a verificar que a proposta recebida de um fornecedor novo (ainda não aprovado) é interessante e poderá ser uma mais valia para a empresa porque é mais competitivo, poderá ajudar a ter maior poder negocial junto dos actuais, o Gestor de Compras contacta a Dir. Qualidade e é despoletado o processo que leva a aprovação do mesmo.	insuficiente		
	Riscos Considerados não aplicáveis ou de Impacto/Probabilidade de Ocorrência reduzida na sequência da análise desenvolvida pela Auditoria Interna								
	32. Acessos		2	N/A	N/A	N/A	N/A	1	1
	40. Reputação	2	2	N/A	N/A	N/A	N/A	1	1
	51. Alinhamento	2	2	N/A	N/A	N/A	N/A	1	1
	52. Contratos/Compromissos		2	N/A	N/A	N/A	N/A		
	57. Orçamento	2	2	N/A	N/A	N/A	N/A	1	1
	59. Avaliação de Investimentos	2	2	N/A	N/A	N/A	N/A		
				N/A	Confirmação dos controlos efectuados pela área da qualidade na recepção dos matérias relevantes para a qualidade	Existe um procedimento da qualidade nas entregas dos materiais. Os materiais são acompanhados por um certificado de garantia da qualidade, e que é entregue na qualidade. A área da qualidade, verifica se está tudo em conformidade e dá o OK, no sistema informático,. Só a partir desta altura é que os materiais são disponibilizados para consumo. Se existir alguma divergência é feita a devolução/reclamação ao fornecedor.	Bom (se aplicado)	2	

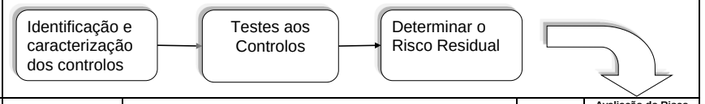
ANEXO 4 - Matriz de Análise de Riscos e Controlos

Fase 4 - Avaliar os Riscos

Grupo de Compras - Materiais de Embalagem

Processo: 1.1. Processo Geral - Compras Orçamento

Fase 4 - Avaliar os Riscos



Sub-processos	Risco						Avaliação do controlo	Avaliação do Risco após análise do controlo	
	Factor de Risco	Imp.	Prob.	Testado (Sim/Não)	Plano de Testes	Resultados dos testes efectuados	Nota	Imp.	Prob.
1.1.4. Criação do Acordo de Fornecimento	**13. Cumprimento, Normas e Regulamentos** Risco de incumprimento de regulamentos e normas externas e internas Risco considerado importante na sequência da análise realizada pela Auditoria Interna, apesar de ter sido classificado inicialmente pelo Gestor como pouco significativo.	-1	-1	Sim	Verificar a existência de Penalidades aplicadas em 2006 à Empresa resultantes de condições contratualizadas	Existência de penalidades aplicadas à Empresa, resultado da aplicação de clausulas contratuais celebrado com um fornecedor. A penalidade é calculada pelo fornecedor e validada pelo gestor de stocks, bem como, as ND emitidas pelo fornecedor.	Suficiente	2	
	15. Cycle Time Risco de actividades irrelevantes e redundantes atrasarem os processos de negócio do Grupo As situações apontadas para a ocorrência deste risco, enquadram-se, na nossa perspectiva no risco de eficiência, pelo que consideramos que o risco Cycle Time terá impacto reduzido nestes processos.	2	2	Sim	Não	Não	Não	Não	Não
	16. Efficiency Risco de ineficiência na satisfação das necessidades dos clientes	2	2	Sim	Inquérito aos gestores relativamente á frequência com que analisam a existência no sistema informático de requisições liberadas aguardando a criação de acordo de fornecimento para o Grupo de Compras	Os compradores analisam (semanalmente) a existência de requisições liberadas no sistema informático e que estão a aguardar a criação de acordo de fornecimento, com o intuito de regularizar as situações.	Bom (se aplicado)	2	1
				Não	Não testado. Não existe evidência	Os compradores contactam a área requisitante pedindo a liberação da requisição de modo a que possam criar o acordo de fornecimento.	Bom (se aplicado)		

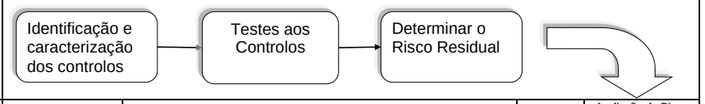
ANEXO 4 - Matriz de Análise de Riscos e Controlos

Fase 4 - Avaliar os Riscos

Grupo de Compras - Materiais de Embalagem

Processo: 1.1. Processo Geral - Compras Orçamento

Fase 4 - Avaliar os Riscos



Sub-processos	Risco						Avaliação do controlo	Avaliação do Risco após análise do controlo	
	Factor de Risco	Imp.	Prob.	Testado (Sim/Não)	Plano de Testes	Resultados dos testes efectuados	Nota	Imp.	Prob.
	26. Authority/ Limit Risk Risco dos colaboradores executarem tarefas que não era suposto ou não executarem as tarefas que lhes estavam atribuídas Risco considerado importante na sequência da análise realizada pela Auditoria Interna, apesar de ter sido classificado inicialmente pelo Gestor como pouco significativo.	2	2	Sim	- Analisar um acordo de fornecimento e verificar se está assinado de acordo com os níveis de autorização definidos internamente.	O acordo com o fornecedor XYZ, não se encontrava assinado de acordo com os níveis de autorização estabelecidos.	insuficiente	2	
	32. Access Risco do acesso à informação /sistemas de informação ser indevidamente concedido ou recusado.	2	2	Não	N/A	N/A	Não Avaliado	2	
	37. Fraude do Colaborador Risco de empregados, clientes ou fornecedores individualmente ou em conluio praticarem fraudes contra a empresa **Considerado risco reduzido neste sub-processo**	1	1					1	1
	Riscos Considerados não aplicáveis ou de Impacto/Probabilidade de Ocorrência reduzida na sequência da análise desenvolvida pela Auditoria Interna								
	11. Interrupção do Negócio	2	2	N/A	N/A	N/A	N/A	1	1
	15. Tempo do Processo	2	2	N/A	N/A	N/A	N/A	1	1
	23.Falha de Produto/serviço	2	2	N/A	N/A	N/A	N/A	1	1
	24. Fornecimento Risco de não existir no mercado o material/serviço com o preço/qualidade desejado pela Unidade de Negócio	2	2	N/A	N/A	N/A	N/A	1	1
	28. Comunicação	2	2	N/A	N/A	N/A	N/A	1	1
	30. Subcontratação	2	2	N/A	N/A	N/A	N/A	1	1
	51. Alinhamento	2	2	N/A	N/A	N/A	N/A	1	1
	52. Contratos/ Compromissos	2	2	N/A	N/A	N/A	N/A		
	55. Reporte normativo	2	2	N/A	N/A	N/A	N/A		

Anexo 5 - Matriz de riscos Residuais do Processo de compras

Fase 4 - Avaliar os Riscos

MATRIZ DE RISCOS (Residuais) PROCESSO: *1.1.2. Processo Geral - Compras Orçamento - Selecção do fornecedor e validação das condições*

RISCOS DO MEIO ENVOLVENTE

	A.I. I	A.I. P
1.Disponibilidade Capital		
2. Perda Castatrófica		
3. Concorrência		
4. Mercados Financeiros		
5. Industria		
6. Legal		
7. Normativo		
8. Sensibilidade		
9. Relações com accionistas		
10. Político		

RISCOS DO PROCESSO

	A.I. I	A.I. P
RISCO OPERACIONAL		
11. Interrupção do negócio	3	1
12. Capacidade		
13. Comprimento normas e regulamentos	2	2
14. Satisfação dos consumidores	2	2
15. Tempo do Processo		
16. Eficiência	3	2
17. Ambiental		
18. Saúde e Segurança		
20. Obsolescencia		
19. Recursos Humanos	2	2
21. Expectativas de Performance		
22. Desenvolvimento de Produto		
23. Falha do Produto/Serviço	3	2
24. Fornecimento		
25. Perda de Valor das Macas		

	A.I. I	A.I. P
RISCO DE AUTORIDADE		
26. Autoridade /Limite Risco		
27. Facilidade de Mudança		
28. Comunicação	2	2
29. Liderança	2	2
30. Subcontratação	1	1
31. Incentivos Performance		

	A.I. I	A.I. P
PROCESSAMENTO INFORMAÇÃO / RISCO TECNOLÓGICO		
32. Acessos	1	1
33. Disponibilidade		
34. Integridade Sistemas de Informação		
35. Infrastructuras		
36. Relevancia da Iinformação		

	A.I. I	A.I. P
RISCO DE INTEGRIDADE		
37. Fraude do Colaborador	2	2
38. Actos Ilegais		
39. Fraude da Gestão		
40. Reputação	1	1
41. Utilização não autorizada		

	A.I. I	A.I. P
RISCO FINANCEIRO		
42. Crédito - Colateral		
43. Crédito - Concentração		
44. Crédito- Escassez		
45. Liquididez - Cash Flow		
46.Liquididez - Concentração		
47. Preço - Câmbio		
48. Preço Capitais Próprios		
49. Preço - Instrumentos Financeiros		
50. Preço - Taxa de Juro		

Legenda
I - Impacto (1 - Gerível; 2 - Importante 3 - Criítico)
P - Probabilidade (1 - Remota; 2 - Possível; 3 - Provável)

	A.I. I	A.I. L
RISCO OPERACIONAL		
51. Alinhamento	1	1
52. Contratos/ Compromissos		
53. Avaliação da Performance (Operacional)		
54. Preço		
55. Reporte normativo (Operacional)		

	A.I. I	A.I. L
RISCO FINANCEIRO		
56. Informação Contabilistica		
57. Orçamento	1	1
58. Avaliação Informação de gestão		
59. Avaliação de investimentos		
60. Fundo de pensões		
61. Reporte normativo (Financeiro)		
62. Impostos		

	A.I. I	A.I. L
RISCO ESTRATÉGICO		
63. Portfólio do Negócio		
64. Avaliação do Ambiente do Negócio		
65. Ciclo de Vida		
66. Organização da Empresa		
67. Avaliação da Performance (Estratégica)		
68. Planeamento		
69. Alocaão de recursos		
70. Valorização		

Fonte: Adaptada da Business Risk Model - Global Best Practices -PricewaterhouseCoopers

Anexo 5 - Matriz de riscos Residuais do Processo de compras

Fase 4 - Avaliar os Riscos

MATRIZ DE RISCOS (residuais) PROCESSO: *1.1.4. Processo Geral - Compras Orçamento - Criação do Acordo de Fornecimento*

RISCOS DO MEIO ENVOLVENTE

	A.I	
	I	P
1.Disponibilidade Capital		
2. Perda Castatrófica		
3. Concorrência		
4. Mercados Financeiros		
5. Industria		
6. Legal		
7. Normativo		
8. Sensibilidade		
9. Relações com accionistas		
10. Polítíco		

RISCOS DO PROCESSO

	A.I.	
	I	P
RISCO OPERACIONAL		
11. Interrupção do negócio	1	1
12. Capacidade		
13. Comprimento normas e regulamentos	2	2
14. Satisfação dos consumidores		
15. Tempo do Processo		
16. Eficiência	2	1
17. Ambiental		
18. Saúde e Segurança		
20. Obsolescencia		
19. Recursos Humanos		
21. Expectativas de Performance		
22. Desenvolvimento de Produto		
23. Falha do Produto/Serviço	1	1
24. Fornecimento	1	1
25. Perda de Valor das Macas		

	A.I	
	I	P
RISCO DE AUTORIDADE		
26. Autoridade /Limite Risco		2
27. Facilidade de Mudança		
28. Comunicação	1	1
29. Liderança		
30. Subcontratação	1	1
31. Incentivos Performance		

	A.I	
	I	P
PROCESSAMENTO INFORMAÇÃO / RISCO TECNOLÓGICO		
32. Acessos		2
33. Disponibilidade		
34. Integridade Sistemas de Informação		
35. Infrastructuras		
36. Relevancia da Iinformação		

	A.I	
	I	P
RISCO DE INTEGRIDADE		
37. Fraude do Colaborador	1	1
38. Actos Ilegais		
39. Fraude da Gestão		
40. Reputação		
41. Utilização não autorizada		

	A.I	
	I	P
RISCO FINANCEIRO		
42. Crédito - Colateral		
43. Crédito - Concentração		
44. Crédito- Escassez		
45. Liquididez - Cash Flow		
46.Liquididez - Concentração		
47. Preço - Câmbio		
48. Preço Capitais Próprios		
49. Preço - Instrumentos Financeiros		
50. Preço - Taxa de Juro		

Legenda

I - Impacto (1 - Gerível; 2 - Importante 3 - Criítico)

P - Probabilidade (1 - Remota; 2 - Possível; 3 - Provável)

	A.I.	
	I	P
RISCO OPERACIONAL		
51. Alinhamento	1	1
52. Contratos/ Compromissos	1	1
53. Avaliação da Performance (Operacional)		
54. Preço		
55. Reporte normativo (Operacional)	1	1

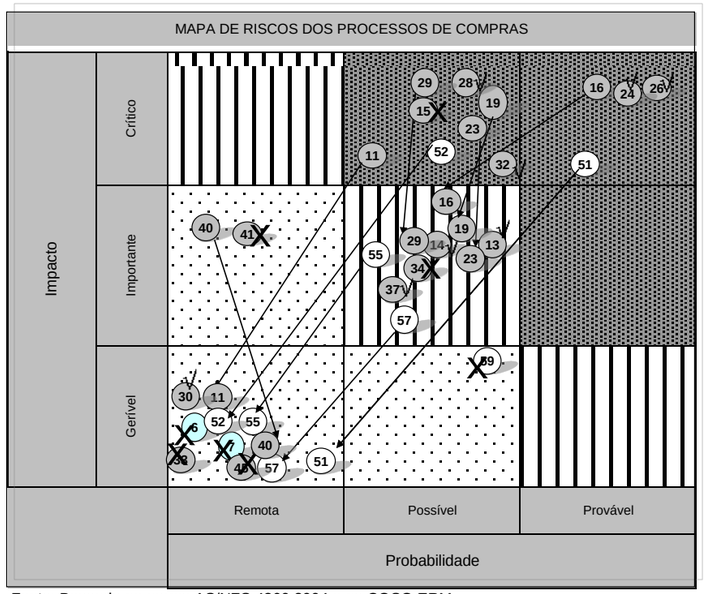
	A.I.	
	I	P
RISCO FINANCEIRO		
56. Informação Contabilistica		
57. Orçamento		
58. Avaliação Informação de gestão		
59. Avaliação de investimentos		
60. Fundo de pensões		
61. Reporte normativo (Financeiro)		
62. Impostos		

	A.I	
	I	P
RISCO ESTRATÉGICO		
63. Portfólio do Negócio		
64. Avaliação do Ambiente do Negócio		
65. Ciclo de Vida		
66. Organização da Empresa		
67. Avaliação da Performance (Estratégica)		
68. Planeamento		
69. Alocaão de recursos		
70. Valorização		

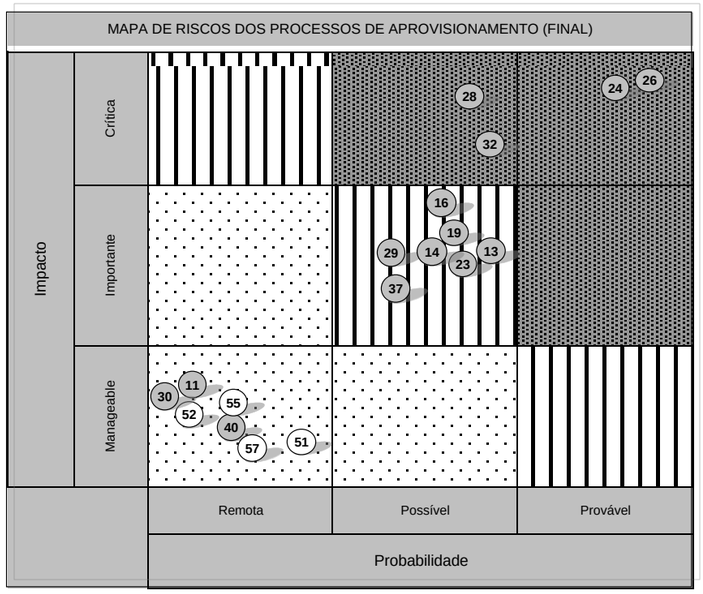
Fonte: Adaptada da Business Risk Model - Global Best Practices -PricewaterhouseCoopers

Anexo 5 - Matriz de Risco Residual do Processo de Compras
Fase 4 - Avaliar os Riscos

Processos / Riscos		11. Interrupção do negócio	13. Cumprimento normas e regulamentos	14. Satisfação do Consumidor	16. Eficiência	19. Recursos Humanos	23. Falha de Produto/Serviço	24. Fornecimento	26. Risco de Autoridade	28. Comunicação	29. Liderança	30. Subcontratação	32. Acessos	37. Fraude do colaborador	40. Reputação	51. Alignhamento	52. Contrato/Compromisso	55. Reporte normativo (Operaconal)	57. Orçamento	Soma dos riscos	% Risco do Processo	Nº Ocorrências Risco Abs. >3	Ranking Processos (Risco Abs. >3)
1.1. Compras Orçamento	1.1.2. Selecção do fornecedor e validação das condições	2	4	4	4	4	4	9	9	6	4	1	1	4	1	1			1	59	69%	10	1
	1.1.4. Criação do Acordo de Fornecimento	1	4	2	2	1	1	1	6	1	1	1	6	1	1	1	1	1	1	27	31%	3	2
Nº Ocorrências		2	2	1	2	1	2	2	2	2	1	2	2	2	1	2	1	1	1				
Nº Ocorrências [Risco Abs. >3]		0	2	1	1	1	1	1	2	1	1	0	1	1	0	0	0	0	0				



Mapeamento



Fonte: Baseado na norma AS/NZS 4360:2004 e no COSO ERM

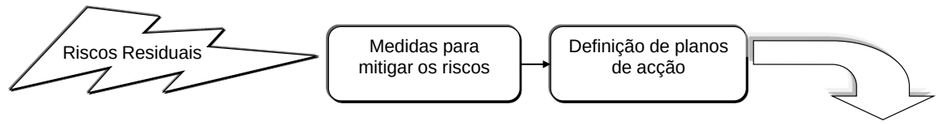
Legenda:

Área menos prioritária - Estes riscos são normalmente aceitáveis, no seu nível actual. As empresas de sucesso eliminam os controlos irrelevantes e redundantes.

Área Intermédia - "Inspeccionar e corrigir" os controlos e monitorizar os processos são medidas adequadas para mitigar os riscos.

Área a precisar de atenção imediata - Elevado Impacto e Probabilidade do risco acontecer. O Objectivo é o de evitar ou prevenir estes riscos na origem.

ANEXO 6 - Matriz de Tratamento de Riscos do processo de Compras
Fase 5 do Modelo de GR - Tratar os Riscos



Avaliação do Risco Residual							
Nº Risco	Designação	Factores de Risco	Estratégia Proposta	Possíveis medidas para procurar mitigar o risco residual	**Plano de Implementação**		
				Medida	**Tarefa**	**Responsável**	**Prazo**
16	Eficiencia	As áreas operacionais não enviam para o Departamento de Compras a informação relativa aos orçamentos atempadamente, ou quando chega é posteriormente alterada, o que pode pôr em causa a recepção de materiais e por conseguinte a satisfação das necessidades dos clientes. Por outro lado, verifica-se situações em que o processo de aprovação de fornecedores é moroso. Ambas as situações atrás referenciadas podem provocar atrasos nas negociações, podendo originar uma perda de oportunidade negocial	Controlar	O Departamento de Compras deverá definir juntamente com as Áreas Operacionais um calendário para a recepção de toda a informação necessária, de modo a evitar atrasos e desta forma comprometer o poder negocial, bem como, deverá ser definida uma equipa de trabalho com todos os intervenientes no processo de aprovação de fornecedores com o intuito de se definirem limites temporais razoáveis de intervenção de cada área por tipo de material.			
24	Fornecimento	A informação solicitada a fornecedores de materiais em que o risco de fornecimento é elevado que permita avaliar a sua capacidade financeira e situação económica não parece ser suficiente podendo conduzir a risco de fornecimento, falha do produto ou eficiência no caso de o fornecedor enfrentar problemas financeiros/económicos significativos.Dependência do know-how (nomeadamente ao nível da manutenção) de entidades que trabalham com a Empresa em regime de Subcontratação, que caso deixarem de trabalhar com a Empresa poderão causar-lhe problemas.	Controlar	Na admissão de um novo fornecedor nacional, sugerimos que se verifique se a firma em causa se encontra na Lista de Devedores ao Fisco disponibilizada no site das Finanças. No caso de fornecedores em que o montante em negociação assume proporções significativas (de acordo com limite a definir pelo Departamento de Compras) ou para materiais críticos, e se perspectivem períodos de fornecimento longos (por exemplo 1 ano), deverá ser ponderada a recolha de informação económico-financeira do fornecedor por recurso a entidades especializadas que fornecem este tipo de informação (ex: Dun & Bradstreet e outras entidades).			
26	Autorizações	Processos de compra em que não existe qualquer documento que justifique a escolha do fornecedor, ou os critérios que estiveram na base dessa decisão, bem como, não existe evidência da aprovação.	Controlar	Entendemos que deve sempre existir um documento justificativo da escolha do fornecedor e evidência da sua aprovação, de modo a garantir que a escolha foi efectuada por pessoa autorizada e a quem está atribuída essa competência. Sugerimos que seja definido um documento modelo obrigatório que contenha os motivos que justifiquem a escolha do fornecedor, documento este que deverá estar arquivado juntamente com o processo de compras. Estes mapas deverão apresentar evidência de aprovação de acordo com os níveis de delegação definidos no documento interno.			
28	Comunicação	Solicitações de cotação efectuadas ao mesmo fornecedor com os materiais repartidos por empresa do grupo. Esta situação leva a que o fornecedor não tenha uma visão consolidada dos materiais e quantidades solicitados para todo o Grupo podendo levar a uma perda de vantagem negocial. Nestas situações o comprador solicita ao fornecedor que veja para as propostas de um modo global.	Controlar	Sugerimos que seja desenvolvida uma ferramenta que permita que uma solicitação de cotação reúna todas as requisições de compra do mesmo material ignorando os campos Empresa permitindo assim que o fornecedor possa ter o resumo total da quantidade encomendada pelo Grupo.			
32	Acessos		A analisar				